SRMGSA

Safety Risk Management Guidance for System Acquisitions Version 2.1

Air Traffic Organization February 2016

ALL POINTS/SAFETY
everyone. everywhere. everyday.

FAA
Air Traffic Organization

Table of Contents

Figures

Tables

Appendices

Preface

This version of the Safety Risk Management Guidance for System Acquisitions (SRMGSA) cancels SRMGSA Version 2.0. It applies to acquisitions that have a potential effect on safety risk in the National Airspace System (NAS) when the acquired systems are operationally fielded. The SRMGSA includes information pertaining to the Federal Aviation Administration (FAA) Acquisition Management System (AMS) changes, Next Generation Air Transportation System (NextGen) Portfolio Management, and Integrated Safety Management. The body of the document contains only high-level policy and guidance concerning Safety Risk Management (SRM) in acquisitions. More detailed guidance on how to conduct specific analyses is contained in the appendices to this document.

For those applying SRM to acquisitions that affect safety risk in the NAS, the SRMGSA is a governing document with which compliance is mandatory. The SRMGSA and all other current Air Traffic Organization (ATO) Safety Management System (SMS) policy and guidance are available on the ATO SMS website. Safety and Technical Training (AJI) is the focal point for determining how system acquisitions affect safety risk in the NAS. AJI is also the Office of Primary Responsibility for the SRMGSA. All questions concerning this document should be directed to 9-AJI-SMS@faa.gov.

1 Introduction

The SRMGSA defines the scope, purpose, objectives, and required activities of the FAA's systems safety effort as it applies to SRM for all system acquisitions that provide Communication, Navigation, and Surveillance (CNS), Air Traffic Management (ATM), and other services in the NAS.[1] The SRMGSA applies to all personnel in the ATO performing safety risk assessments on system acquisitions and is of interest to those performing a similar role for the Assistant Administrator of the Office of NextGen (ANG), the Office of Airports (ARP), or other FAA Lines of Business (LOBs).

The SRMGSA embodies and contributes to the spirit of the FAA's safety culture. A positive safety culture places a pervasive emphasis on safety and promotes:

- An inherently questioning attitude,
- A resistance to complacency,
- A commitment to excellence,
- The involvement and accountability of management, and
- The fostering of personal accountability and corporate self-regulation in safety matters.

1.1 Purpose

The purpose of the SRMGSA is to meet the requirements of and implement the policy stated in Section 4.12 of the AMS. Section 4.12 requires the application of an SMS, referring to the ATO SMS Manual and the SRMGSA as governing documents with which compliance is mandatory. Thus, the SRMGSA provides the guidelines that must be used by the ATO and other organizations when conducting SRM in acquisitions. In addition, FAA Order 1100.161, A*ir Traffic Safety Oversight*, focuses the Air Traffic Safety Oversight Service's (AOV's) oversight efforts on the acquisition and implementation of new systems. Per AOV Safety Oversight

1. For a complete definition of NAS services, refer to the NAS Requirements Document. This is the source of functional and performance requirements for FAA systems that provide air traffic control services. All operational systems' capabilities are traceable to specific requirements in the NAS Requirements Document. This document may be found at the NAS Enterprise Architecture (EA) Portal.

Circular (SOC) 09-11, *Safety Oversight*, new acquisitions are required to follow the guidance of the FAA AMS and meet the program requirements defined in the ATO SMS Manual and the SRMGSA.

The conduct of SRM maintains or improves the safety of the NAS by identifying the safety risk associated with making NAS changes and providing that input to decision makers responsible for managing and mitigating this safety risk. When system[2] safety hazards are identified, the subsequent mitigations that are derived from the SRM process (as described in the ATO SMS Manual) are translated into requirements for the acquired systems. In order to assess the safety affects identified in the SRM process, the requirements must be connected to the verification and validation processes.[3] Without these connections, the true residual risk cannot be determined.

The SRMGSA provides a framework and further process definition to execute SRM throughout the entire lifecycle of a system or product. This framework is made formal in the Program Safety Plan (PSP) developed for a program by a Program Safety Team (PST). (Refer to Appendix A for guidance on developing and implementing PSPs and Section 4.5 for more information on PSTs). The SRMGSA follows systems engineering principles to achieve the SRM objectives defined in the various FAA/ATO orders listed in Section 3.

The SRMGSA defines the ATO's processes for effectively integrating systems safety[4] into system changes and NAS modernization in accordance with FAA orders, the ATO SMS Manual, and AMS policy.[5] It describes the AMS phases, organizational roles and responsibilities, program requirements, tasks, monitoring, and reporting requirements associated with performing SRM within the ATO and other organizations involved in acquisitions that affect the NAS (e.g., Office of Aviation Safety (AVS), ARP, and ANG).

The SRMGSA provides the following:

- Safety management guidance for acquisitions during the following phases of the AMS lifecycle:
    - Concept and Requirements Definition (CRD),
    - Investment Analysis (IA),
    - Solution Implementation (SI), and
    - In-Service Management (ISM).
- SRM in support of agency Risk-Based Decision Making (RBDM).

2. Per the FAA Systems Engineering Manual (SEM), a "system" can be defined in numerous ways. The International Council on Systems Engineering (INCOSE) Handbook defines a system as "a combination of interacting elements organized to achieve one or more stated purposes." The SEM states, "A system is an integrated set of constituent pieces that are combined in an operational or support environment to accomplish a defined objective. These pieces include people, hardware, software, firmware, information, procedures, facilities, services, and other support facets."

3. . The FAA employs verification and validation throughout the acquisition management lifecycle in accordance with AMS verification and validation guidelines to support investment decisions and approvals. Verification ensures a product is built right according to specifications. Validation ensures the right product is built (fulfills its intended use). Verification and validation are performed early and incrementally throughout the lifecycle management process on select work products, product components, and products. See AMS Section 2.1.6 for more information.

4. Systems safety is the process for designing safety into a product through the engineering process using a systematic approach.

5. The Assistant Administrator for ANG also uses the SRMGSA to guide his or her activities when conducting SRM.

- Specific guidance for system changes.
- An overview of the Joint Resources Council's (JRC's) expectations regarding SRM.

The SRMGSA describes the organization and responsibilities of FAA management, the ATO, and ANG for fulfilling SRM objectives. It also addresses AJI's relationship within the ATO (specifically with the Program Management Organization (PMO) and the Service Units) and with ANG for developing and approving safety documentation and accepting risk prior to JRC decisions.

The SRMGSA is supplemented by the following ATO Safety Guidance (ATO-SG) documents:

- ATO-SG-14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;
- ATO-SG-14-02, *Software Assurance Approval Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;
- ATO-SG-14-03, *Conducting a DO-278A Software Assurance Compliance Gap Analysis for Acquired NAS Systems*; and

When a change affects the accepted scope of performance or requirements, the SRMGSA may be revised upon agreement among AJI, the PMO, the ATO Chief Safety Engineer, and the Acquisition Systems Advisory Group.

1.2 Scope

The SRMGSA supports the goals of the AMS process with guidance focused on service delivery and an improved transition of programs from research and development to implementation.[6] AMS policy, FAA/ATO orders, and the ATO SMS Manual mandate a planned and organized SRM approach to RBDM that is consistent with the role of each organization in the FAA.

Leadership, direction, and guidance relating to FAA acquisition policy, research, system development, and agency information resource management require continuous collaboration among ATO organizations, ANG, and other LOBs. This requires shared accountability and responsibility as these organizations engage throughout the system lifecycle. The SRMGSA encourages this collaboration, particularly within the areas of requirements management, acquisition policy, and systems safety.

NAS systems not acquired through the FAA AMS process (e.g., acquired by other governments, Eurocontrol, or the Department of Defense) are outside the scope of the SRMGSA. However, they are within the scope of the FAA SMS and must follow the requirements of the ATO SMS Manual before they can be fielded. This includes system constituent pieces like leased services/ vendor-provided services that affect the safety of the NAS.

The SRMGSA briefly discusses the assessment of proposed NAS initiatives (i.e., pre-acquisition efforts) in support of agency RBDM. An initiative can be defined as any high-level change to the

6. SRM related to the ISM phase is limited to the implementation of the system. The ATO SMS Manual provides guidance for changes to baselined systems.

operation of the NAS. The FAA Administrator may direct that any initiative be assessed for safety. This may include NextGen priorities, proposed capabilities, or other types of changes being considered in the agency. Safety risk assessments for initiatives are integrated in nature and entail the review of risks induced by the impact of and interdependencies among multiple planned or fielded NAS systems. Initiatives may pose new safety risks, decrease existing risks, or impact the current risk profile of existing NAS systems and operations. Recommendations are developed as to whether the initiative should be pursued, redefined, or canceled based on the results of the integrated safety analyses.

2 Safety Management Policy

2.1 Acquisition Management

AMS Section 4.12 in the FAA Acquisition System Toolset (FAST) contains the AMS policies for the safety management of NAS acquisitions. This section requires that:

- Safety management be conducted and documented throughout the lifecycle of a system,
- SRM be used to identify safety risks in the NAS,
- Product development be conducted at a rigor commensurate with the severity of the hazard that would result from a failure of the product, and
- Non-developmental product changes be aligned with the intent of SMS policy during "developmental acquisition" (i.e., qualification testing of commercial-off-the-shelf (COTS) items but not design reviews).

2.2 System Safety

System Safety is a standardized management and engineering discipline that integrates the consideration of human, machine, and environment in planning, designing, testing, and maintaining operations, procedures, and acquisition projects. System Safety is applied throughout a system's entire lifecycle to achieve an acceptable level of safety risk within the constraints of operational effectiveness, time, and cost.

The Program Manager (PM) of any acquisition project must institute a system safety program that meets the requirements of the ATO SMS. The status of system safety must be presented at all decision points and investment reviews. Detailed guidelines for safety management and development assurance are found in the FAST; the ATO SMS Manual; RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*;[7] and the ATO-SG documents[8] referenced in this document.

2.3 Integrated Safety Management

The highly distributed and interconnected nature of the NAS and NextGen in particular presents complex safety challenges to the NAS. In addition, many changes to the NAS necessary to implement NextGen initiatives may occur in a parallel or overlapping manner. The past SRM

7. An RTCA user identification and password are required to down load RTCA documents. FAA employees may obtain an RTCA membership username and password by contacting RTCA, Inc.

8. See the current version of ATO Order JO 1030.1, *Air Traffic Organization Safety Guidance*, for information concerning the ATO-SG program.

paradigm was focused on analyzing individual changes; it was insufficient for addressing all the hazards identified as a result of these planned interactions and interconnectivity.

The legacy NAS is a "System of Systems," providing multiple services to users. The NAS is evolving into an even more complex configuration. Future acquisitions are beginning to blur the lines of a "system" with defined/fixed boundaries and interfaces. Systems, programs, and projects no longer have unique or exclusive functionality. In fact, the functionalities not only overlap but may build on one another, subsume each other, or combine for a joint function or capability. This perspective was not considered historically, but is important to applying the concept of integrated safety in acquisitions. Integrated Safety Management must be performed to assess risks of initiatives in support of agency RBDM.

Integrated Safety Management represents a more robust, holistic, and integrated approach to performing safety analysis. Integrated Safety Management uses existing safety policy and methodologies, as well as systems engineering processes. It is a critical component not only for successfully achieving the NextGen vision, but for all enhancements to the NAS.

Directionality is a critical aspect of Integrated Safety Management. Safety assessments using Integrated Safety Management principles must be conducted in three "directions": vertical, horizontal, and temporal:

- Vertical Integration ensures the consistency of safety assessments across hierarchical levels from the program or system level up to the NAS level. It essentially is a look "up" the NAS at Enterprise-level / project-level architectural alignment.
- Horizontal Integration ensures that the interactions and interdependencies across organizations, operational capabilities, portfolios, operational improvements (OIs), increments, current operations, and individual programs or systems are addressed in safety assessments. It is essentially a look "across" the NAS at project-level, inter-architectural alignment, linkages, and interdependencies.
- Temporal Integration ensures that the impacts of hazards and their associated mitigations across implementation timelines are understood and taken into consideration. It is a look at the impact of phased implementations of NAS initiatives.

Identifying hazards and assessing safety risk remains the basis of all safety management efforts for FAA programs. Integrated Safety Management does not change the basic SRM process; it expands the perspective of the required analysis and uses existing elements of the FAA's systems engineering process to ensure that no safety gaps occur as aviation capabilities are developed and implemented in the NAS.

2.4 Safety Performance Targets and Monitoring Plans

Safety performance targets are used to assess safety performance with respect to existing controls and newly implemented safety requirements after a NAS change is operationally fielded. A system that is acquired is typically a key component of any operational change and thus part of that change's safety performance targets and monitoring plans.

For acquisition programs, monitoring responsibilities end when all activities outlined in the Safety Risk Management Document Monitoring Plan and the safety section of the Post-Implementation Review Plan are complete. After the In-Service Decision, additional safety

requirements may be identified via an operational assessment, a Post-Implementation Review, or other means that could result in design changes to the system."

Refer to the ATO SMS Manual for more information on safety performance targets and monitoring plans.

2.5 Software-Intense Systems

Software-intense systems must demonstrate that a software product was developed at an appropriate level of rigor. The establishment of a development assurance program in accordance with RTCA DO-278A is one acceptable means[9] of demonstrating this level of rigor.[10] See Section 6.3 for additional details.

3 References

The current versions of the following FAA/ATO orders and guidance documents supplement the SRMGSA:

- The ATO SMS Manual;
- The FAA AMS Policy / FAST;
- ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*;
- ATO Order 8040.4, *Safety Risk Management*;
- FAA Order 1100.161, *Air Traffic Safety Oversight*;
- FAA Order 6032.1, *National Airspace System (NAS) Modification Program*;
- ATO Order JO 1030.1, *Air Traffic Organization Safety Guidance*;
- ATO Order JO 6000.50, *National Airspace System (NAS) Integrated Risk Management*;
- AOV SOC 09-11, *Safety Oversight*;
- AOV SOC 07-02, *AOV Concurrence/Approval at Various Phases of Safety Risk Management Documentation and Mitigations for Initial High-Risk Hazards*;
- AOV SOC 07-05, *AOV Guidance on Safety Risk Modeling of High-Risk Hazards*; and
- RTCA DO-278A
- FAA AMS Lifecycle Verification & Validation Guidelines.

4 Roles and Responsibilities

The organizational roles and objectives involved in the AMS SMS are designed to ensure that the following objectives are met:

- Systems under consideration for inclusion in the NAS are evaluated systematically (i.e., from vertical, horizontal, and temporal perspectives) and at an appropriate time to assist in decision-making.

9. Subject to approval by the ATO Chief Safety Engineer, a developer's internal procedures may also suffice.
10. The software development assurance process is covered by ATO-SG-14-02.

- Initiatives are assessed by conducting Integrated Safety Management in support of agency RBDM; results are incorporated into the SRM activities for individual systems, as appropriate.
- Appropriate safety requirements consistent with the AMS are developed for each solution and best systems/safety engineering practices are used in the earliest possible phases of system development.
- Safety performance targets and monitoring plans are established and monitoring activities are conducted in accordance with the ATO SMS Manual.
- Hazards are identified and assessed for safety risk.
- Safety risks are actively controlled and mitigated to an acceptable level, as necessary.
- Consideration of safety risk, an integral part of each AMS decision, is required for every JRC decision in which resources are committed to the development and acquisition of systems.
- FAA resources are properly focused on controlling and mitigating the highest risk elements and hazards of the NAS and the systems under development.
- Integrated Safety Management is conducted to provide a complete picture of the potential safety risks of fielding a particular NAS capability (see Sections 4.2 and 4.4).

To accomplish these objectives, any organization proposing a change to the NAS must commit the necessary resources to ensure that all required safety analyses and documents are completed.

The roles and responsibilities of each organization involved in implementing the AMS in system acquisitions are detailed below. A complete description of roles and responsibilities for the JRC and organizational entities can be found on the FAST website.

4.1 JRC Secretariat

The JRC Secretariat maintains the AMS-based JRC Readiness Criteria Checklist, which ensures that the appropriate SRM documents required for all investment decision have been coordinated with AJI. The ATO Chief Safety Engineer determines the completion of SRM documentation for programs progressing through the FAA AMS and advises the JRC Secretariat as to his or her decision.[11]

4.2 Assistant Administrator for ANG and NextGen Portfolio Management

NextGen Portfolios are typically organized into OIs, Current Operations,[12] increments, and procedure and documentation changes, all of which must be combined to deliver the required services and capabilities. To provide a complete picture of the potential safety risk of fielding a particular capability (e.g., an OI), Integrated Safety Management must be conducted across that capability. The ANG NextGen Investment Portfolio Leads are responsible for all aspects of their portfolio, including the conduct of Integrated Safety Management.

11. The SRM documentation is not forwarded to the JRC Secretariat for review. The JRC Secretariat only requires a notification from the ATO Chief Safety Engineer that the program has met its SRM obligations, as required by the AMS.

12. A Current Operation is a fielded activity needed to sustain NAS services.

Some portfolios may have more than one FAA organization responsible for implementing their capabilities. ANG obtains work scope agreements from the operational Service Units (e.g., Air Traffic Services (AJT) and System Operations Services (AJR)) through the PMO. Mission Support Services (AJV) supports NextGen Portfolios (especially the validation of complete sets of requirements) during the CRD phase and brings together AJR/AJT inputs. The PMO provides transitional support during the IA phase and full control of the SI phase, and Technical Operations Services (AJW) provides support during the ISM phase.

In general, the SRM work at the solution, procedure, and document change levels is conducted by the PMO, AJV, and AJW following the SRM process described in the ATO SMS Manual. However, at the capability level, the ANG NextGen Investment Portfolio Leads have the responsibility for ensuring the conduct of safety assessments. The Portfolio Leads typically seek the assistance of the ANG Office of Engineering Services, the PMO, and AJI in conducting these assessments. In the conduct of Integrated Safety Management, it is particularly important to properly set the scope of the safety assessments, as there are numerous complex relationships among systems, procedures, OIs, and Current Operations. The scope of a safety risk assessment at this level must be broad enough to include all potentially interacting functions, procedures, and airspace and system components. As such, the NAS EA should set the scope, which also supports tracing analysis results to NAS EA elements. Such traceability to NAS systems, functions, operational activities, etc., facilitates follow-on Integrated Safety Management efforts.[13]

To develop safety assessments with these broader scopes, the ANG NextGen Investment Portfolio Leads must:

- Understand and document all pertinent limitations, constraints, dependencies, assumptions, and performance shortfalls to funnel the free flow of desires into achievable capability shortfall statements worthy of mission and service analysis;
- Ensure that capabilities under consideration are analyzed early (i.e., prior to the Investment Analysis Readiness Decision (IARD)) for possible safety ramifications due to integration with other NAS components;
- Identify how the magnitude of the safety issues/concerns identified early in capability development may impact the way the capability is considered for further investment and development;
- Support the transition of the capability to an implementing organization within the ATO, resulting in an SMS-compliant Operational Safety Assessment (OSA) prior to the IARD; and
- Gather data on, understand, and articulate the safety issues/concerns as a capability evolves and moves through the acquisition lifecycle.

4.3 Office of Aviation Safety

AVS includes AOV, which oversees the SRM process for system-oriented safety standards related to the acquisition and implementation of new systems in accordance with the current

13. The purpose of the NAS EA is to establish the foundation from which evolution of the NAS can be explicitly understood and modeled.

versions of FAA Order 1100.161 and AOV SOC 09-11.[14] It is important to note that AOV must approve any mitigations identified in an SRM document that lower the safety risk of any initially identified high-risk hazard before those mitigations may be implemented and the system(s) fielded.

4.4 Safety Collaboration Team

The NAS Safety Collaboration Team (SCT) fosters collaboration among safety stakeholders across the FAA LOBs and Staff Offices (SOs) to:

- Perform SRM on planned NAS initiatives;
- Identify and raise awareness of safety issues that span LOBs/SOs through integrated safety analysis;
- Support the advancement and common understanding of Integrated Safety Management;
- Develop common methodologies and maintain lessons learned for conducting Integrated Safety Management; and
- Enhance RBDM for planned NAS changes (e.g., new system acquisitions, processes, policies, procedures, NAS Change Proposals, legacy system enhancements, or unmanned air traffic control towers).

The SCT serves as the technical advisory body to the FAA SMS Committee. The SCT's primary function is to facilitate the Integrated Safety Management of planned NAS changes, particularly when the impact of the planned change crosses LOBs, as directed by the FAA SMS Committee and in accordance with the current FAA Order 8040.4. This is most likely early in the planning stages of a proposed initiative and possibly before the need for a new system acquisition has been identified. Additionally, the SCT may facilitate the identification and analysis of enterprise-level system safety issues within the NAS environment. This could include the development of safety assessments or safety analyses, the results of which can be used as preliminary input data for the safety risk analysis of new system acquisitions.

The SCT may form workgroups (e.g., Safety Analysis Teams or sub-teams) to conduct safety analyses of planned NAS changes (as selected by the FAA SMS Committee) or to conduct assessments. ATO Subject Matter Experts (SMEs) and other safety professionals may be asked to be members of these workgroups. The processes and procedures used by these workgroups and the SCT are beyond the scope of the SRMGSA and will be defined in a separate document.

4.5 Program Safety Team

A PST is a resource provided by the program office to support the safety efforts of the acquisition throughout the AMS lifecycle. The PST may consist of a single safety Point of Contact (POC) or a team of safety experts, depending on the size and complexity of the program.

14. This SOC provides systems-oriented information and guidance material that may be used by the ATO to develop and implement procedures to comply with FAA Order 1100.161.

The PST, in conjunction with the AJI Safety Case Lead (SCL), defines the planned safety effort and ensures that the required safety products are prepared to support the JRC decision process.

The PST must:

- Provide a central POC to coordinate all safety analyses throughout the program's lifecycle;
- Participate in the Safety Strategy Meetings (SSMs), as needed, to determine the safety effort required in support of the AMS milestone decisions;
- Support the safety analyses in accordance with the guidelines in the AMS FAST, the ATO SMS Manual, ATO-SG documents, and this document;
- Submit the proposed PSP and completed SRM documents to the AJI SCL for review and coordination to ensure timely decisions in support of JRC milestone decisions;
- Enter safety tracking and monitoring data into the Safety Management Tracking System (SMTS);
- Ensure that safety assessment and analysis results are addressed in program planning and requirements documents;
- Ensure that any safety issues identified by SCT activities are incorporated into program safety efforts;
- Ensure that any requirements developed as a result of the safety analyses are included as discrete requirements in the preliminary Program Requirements Document (pPRD), the initial PRD, or the final PRD;
- Ensure that the safety requirements are traceable back to identified safety hazards;
- Verify that the mitigations identified to reduce safety risk are included as validated and verified safety requirements in the final SRM document;
- Support the establishment of traceability between safety analysis results and the NAS EA;
- Maintain safety documentation throughout the system lifecycle;
- Include SRM results in investment decision briefings to the JRC; and
- Coordinate the peer review process with the SCLs.

4.6 Air Traffic Organization

4.6.1 Service Unit Roles and Responsibilities

Depending on the acquisition phase of the program, the PMO, AJV, or AJW has the responsibility of ensuring that SRM has been conducted and the necessary documentation has been prepared. They are supported as appropriate by SMEs from AJR, AJT, and/or AJW. Safety professionals within AJI also support the PSTs in preparing the safety documents and representing their functional discipline at reviews with the ATO Chief Safety Engineer. The Service Unit representatives to the PSTs ensure that the Service Unit Vice Presidents are informed of the risks involved in a proposed change to the NAS and recommend that they approve SRM documentation and accept risk, as necessary, in accordance with the ATO SMS Manual.

Specifically, AJV's role is to break down the FAA's Concept of Operations (ConOps) into operational needs. These operational needs are then aligned with new/existing OIs or Current Operations and prioritized and allocated to portfolios. The operational needs are broken down into initial operational requirements, including safety requirements, which may or may not result in a need for an acquisition. AJV validates complete sets of functional, design, and performance requirements for the PMO.

The NAS EA contains roadmaps that describe the transition from the "as is" to the "to be" environment. Roadmaps align the FAA's mission, benefits, and capabilities in relation to its investments. Within the ATO, the PMO coordinates the EA support effort for all roadmaps (except the safety roadmap) by providing the alignment of systems and technologies with the mission/business leads. This includes planning for the application of the SMS in all ATO-managed acquisition programs. The EA also contains architectural "as-is" and "to-be" views that govern the expected architecture, threaded features, levels, functional flow, dependencies, and holistic performance of the NAS to be allocated among integral groups of dependent NAS systems. EA views, more so than roadmaps, help control the impacts of change among NAS systems.

The PMO is responsible for monitoring safety requirements of acquisition programs to ensure the requirements are met through design audits, developmental and operational tests and evaluations, and performance checks (most notably before the Initial Operating Capability (IOC) and the Post-Implementation Review (PIR)).

4.6.1.1 Program Management

Many functions performed by successful acquisition PMs are beyond the scope of the ATO SMS and this document. However, some of these functions are relevant to fulfilling the SRM requirements as they relate to acquiring new solutions. Among them is planning and resource management, which includes ensuring that SMS considerations are part of the decision-making process. Whether SRM is a collateral duty of one person or performed by a PST, the PM must ensure that SMS policy and guidelines are followed.

When forming a safety team, the PM should choose people who are able to:

- Communicate with program stakeholders,
- Understand program objectives,
- Understand program plans and acquisition strategy,
- Develop strategy and action plans for the safety compliance of the program,
- Define safety input into program plans and supplier agreements,
- Perform safety analyses,
- Track and analyze safety compliance for the program,
- Implement mitigation steps as required, and
- Report program safety activity and monitoring results.

4.6.2 ATO Chief Safety Engineer

The primary function of the ATO Chief Safety Engineer is to provide safety leadership and expertise to ensure that:

- Operational safety risk in the air traffic services that the ATO provides to the NAS is identified and managed and

- Safety risk is considered and proactively mitigated in the early development, design, and integration of solutions and across organizations to support NextGen capabilities.

The ATO Chief Safety Engineer must:

- Represent the ATO in resolving high-level safety issues in air traffic operation and decision-making meetings;
- Review and approve SRM documentation associated with NAS changes that require AOV approval, as defined in FAA Order 1100.161;
- Review and approve SRM documentation for acquisition programs and safety assessments for changes done at the national level, as defined in the ATO SMS Manual and the SRMGSA;
- Review and approve safety input in support of JRC investment decisions, as required;
- Serve as the ATO safety focal point for collaboration with the ANG and the PMO on NextGen transitional activities;
- As requested by the SCT, assess reports presented to ensure that safety findings are representative of actual safety concerns and safety risks involved as the initiative matures;
- Ensure that the safety case management process includes Integrated Safety Management to ensure a comprehensive safety review of concepts, solutions, systems, and procedures;
- Provide the Director for Policy and Performance and the Vice President of AJI with senior-level input on ATO safety-related issues for air traffic operations, acquisitions, and second level engineering;
- Review and approve proposed changes to safety policy and guidance for incorporation in ATO Order JO 1000.37, the ATO SMS Manual, and the SRMGSA;
- Collaborate with internal and external stakeholders to facilitate mitigation of safety risks that cross LOBs; and
- Approve RTCA DO-278A (or equivalent document) lifecycle data.

4.6.3 AJI Roles and Responsibilities

AJI is the ATO's focal point for safety. It provides the ATO with safety direction while driving the SRM / Integrated Safety Management process. AJI also coordinates the EA support efforts on the safety roadmap for the ATO.

4.6.3.1 AJI Safety Engineering Team Manager

For new SRM efforts related to acquisitions and capabilities, the AJI Safety Engineering Team, AJI-314, Manager is the first AJI POC for Program and Portfolio Managers. The AJI-314 Team Manager manages the safety case workload for a team of safety engineers and assigns an AJI SCL to work with an individual program or initiative based on resource availability. He or she ensures that SRM documentation and software assurance compliance data (e.g., RTCA DO-278A or related lifecycle data) is processed in accordance with the ATO SMS Manual, relevant ATO-SG documents, and the SRMGSA before being submitted to the ATO Chief Safety Engineer for approval and signature.

The AJI-314 Team Manager must:

- Assign an AJI SCL to work with a PST;
- Balance the workload among AJI SCLs, considering commonality with existing assignments, their experience and expertise, and program and portfolio complexities; and
- Confirm that any documentation being submitted to the ATO Chief Safety Engineer for approval has been developed and peer reviewed in accordance with the SRMGSA and internal AJI processes.

4.6.3.2 AJI Safety Case Leads

The AJI SCLs (or their designees) are experts in SRM policy and guidance that pertains to the AMS. The AJI SCLs assist the PSTs responsible for conducting or managing systems safety programs. The AJI SCLs are the ATO's acquisition safety focal points and ensure that each safety product associated with an AMS milestone is peer reviewed; they ensure that all resulting comments and concerns are addressed prior to the program's planned AMS decision. The AJI SCLs must:

- Meet with the PSTs and convene SSMs, as needed, to ensure timely development of SRM documentation in support of JRC milestones, starting in the CRD phase and ending during the ISM phase.
- Work with a PST, when assigned by the AJI-314 Team Manager, to guide the team in conducting and developing the safety analyses and the PSP. As the SRM documentation is being developed, the AJI SCLs provide periodic feedback to the PST. At the appropriate time, they recommend to the AJI-314 Team Manager that the SRM documentation is ready to enter the peer review process for approval and signatures.
- Coordinate the peer review of SRM documentation with the PST (see Section 8.4) within a timeframe that is consistent with the planned JRC decisions. This review must, at a minimum, ensure that the cause and effect relationship between proposed changes to the NAS and the risks to the operational safety of the NAS are explicitly analyzed and documented.
- Serve on SCT-chartered teams as requested to represent the entire ATO from a safety perspective.
- Ensure that safety risks associated with initiatives that have conducted safety analyses/assessments are mapped to and considered in the SRM activities of any acquisition program.
- Identify, evaluate, and document lessons learned.

4.6.3.3 Independent Safety Assessment Team

The AJI Independent Safety Assessment (ISA) Team is responsible for evaluating designated acquisition systems (and major modifications) through the Independent Operational Assessment (IOA) function.[15] To ensure that solutions are within acceptable levels of safety risk, the ATO SMS and the AMS require that IOAs be conducted on designated systems prior to the ISD to identify safety hazards and operational concerns in a representative operational environment.

15. See AMS Section 4.5 for more information.

During the ISM phase, the ISA Team is also responsible for conducting post-implementation safety assessments of designated systems, procedures, and service capabilities to independently assess the residual risk of changes in the NAS, identify any new hazards or operational concerns not anticipated during SRM, and ensure the mitigations for identified hazards have been properly implemented and comply with SMS requirements.

If new safety hazards are identified, the PMO, working with the AJI SCL, may have to reconvene SRM panels to analyze and assess these hazards.

4.6.4 Roles and Responsibilities Summary

Figure 4.1 summarizes the ATO's safety roles and responsibilities. Refer to Table 9.1 to see which organization is typically responsible for conducting the various safety analyses.

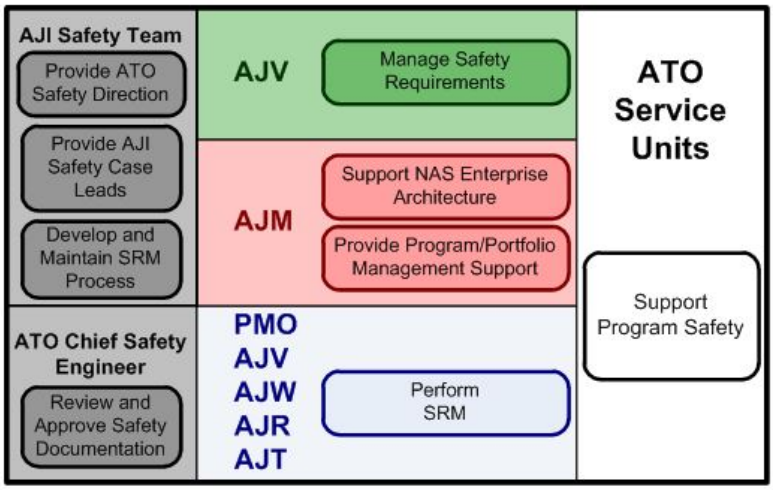

Figure 4.1: ATO Roles and Responsibilities

5 Safety Planning for Acquisitions

5.1 Portfolio Safety Strategy

As described in Section 4.2, the ANG NextGen Investment Portfolio Leads are responsible for ensuring the conduct of Integrated Safety Management within their portfolio. This is not an independent effort; ANG needs to rely on the input of AJI to fully assess the safety posture of any portfolio and to plan Integrated Safety Management efforts. At a high level, AJI supports ANG and NextGen Integrated Safety Management by participating in safety assessments and other SCT-directed safety analyses as requested. AJI also provides consolidated ATO safety review of NextGen planning documents. AJI support also includes:

- Collaborating with ANG on all aspects of NextGen Integrated Safety Management to ensure that safety artifacts are developed as needed during the pre-investment phases of the AMS;[16]
- Developing a single ATO safety strategic plan to support NextGen concepts and implementation as depicted on the NAS EA safety roadmap, as well as tracking ATO Safety Decision Points on the EA safety roadmap;

16. The ANG thrust is prior to the CRD and the IA phases of the process.

- Approving the scope of NextGen safety assessments conducted in the pre-investment phase;
- Participating in safety assessments and other SCT-directed safety analyses as requested;
- Reviewing and approving SRM documents for the NextGen solutions;
- Reviewing and approving safety OIs' functionality and implementation dates in the NextGen Safety Portfolio; and
- Attending technical meetings between ANG and the program offices to coordinate safety program requirements and engineering architecture artifacts.

In addition, AJI and the PMO work with the ANG NextGen Investment Portfolio Leads to identify any Integrated Safety Management gaps that may exist within a portfolio.

5.2 Safety Strategy Meetings

Acquisition strategies vary among investment programs. As a result, the SRM documentation requirements may also vary. The PMO/PST should contact AJI to schedule an SSM to determine the appropriate documentation requirements and for guidance in fulfilling their SRM obligations for the AMS milestone being sought. The AJI SCL facilitates the SSM, contributes their knowledge of policies and SRM practices, establishes peer review process guidelines, and ensures that the proceedings are captured in the meeting minutes. The SSM should be conducted in consultation with the ATO Chief Safety Engineer, if necessary, and particularly if extensive documentation tailoring is planned.

The SSM can be held at any time per the request of the program office, from project inception through the fielding of the system (including prior to the IOC being declared). However, in order to gain the maximum benefit to the program, the SSM should occur early enough in the process to schedule SRM documentation development, review, coordination, and necessary approvals prior to the investment milestone decision point. SRM is a required checklist item for the IARD, the Initial Investment Decision, the Final Investment Decision, and ISD.

The PMO must use the program-specific PSP approved by the ATO Chief Safety Engineer to determine which safety assessments must be conducted during a systems acquisition and which safety requirements must be fulfilled before system deployment. If documented in an approved PSP, the PMO may use alternative methods other than those described in the appendices to capture required information. Also, if documented in an approved PSP, the PMO may prepare a combined analysis (i.e., a combined System Hazard Analysis (SHA) / Sub-System Hazard Analysis (SSHA)) or bypass analyses entirely to meet the AMS requirements.

In addition to the overall safety strategy, the PSP and any other SRM products (OSA, Comparative Safety Assessment (CSA), etc.) may be discussed. Meeting minutes containing the strategy agreed upon for satisfying acquisition SRM requirements must be produced for each SSM.

The ANG Enterprise Safety and Information Security Services Division is an invited participant to all SSMs. For SSMs held for programs in or about to enter the CRD phase, the PMs must consult with the ANG CRD lead before the SSM convenes.

Sometimes, acquisition strategies change or there is not enough information available to determine the SRM documentation requirements for the entire acquisition lifecycle. If so, additional SSMs can be scheduled as often as is necessary.

6 Other Considerations

6.1 Baseline Change Management

For any acquisition program under its jurisdiction, the JRC approves and baselines all required AMS program documents (i.e., PRDs, acquisition program baseline, business cases, and Implementation Strategy and Planning Documents). It may also make acquisition program baseline change decisions that alter program performance, cost, and schedule baselines during SI for investment programs. From an SRM viewpoint, if a baseline change is being proposed, the PMO/PST may need to review and update the PSP and any safety assessments that have already been completed to ensure that the new baseline does not impact the risk mitigation strategies already identified. If it does, then the predicted residual risks identified in the completed safety assessments may not be achievable, and the new predicted residual risk without these mitigations implemented may be unacceptable.

A baseline change could affect the risk mitigation strategies already identified in the following ways:

- If the program cost is being re-baselined, the proposed new budget may not include funding to implement the mitigations previously identified.
- If the schedule is being re-baselined, the proposed new schedule may impact the temporal aspects of the identified risk mitigation strategy. In other words, the planned mitigations may not be in place as expected and required.
- If the performance is being re-baselined, the new requirements may be sufficiently different that the assumptions made and analyses conducted as part of previous safety assessments may no longer apply to the point that previously identified risk mitigation strategies are no longer valid.

6.2 Program Safety Requirements for Decommissioning and Disposal

Disposal of an asset or program is part of the AMS process in the ISM phase and, as such, requires adherence to the SMS as part of its lifecycle management. In addition, decommissioning of a service provided by a program asset targeted for disposal could occur much earlier than the actual disposal and must also meet all of the SMS requirements. Programs or assets facing disposal often have their SMS requirements met by the program or asset replacing them, but this is not always the case.[17] Prior to an asset or program being decommissioned and/or disposed of, the PMO should contact the AJI SCL to convene an SSM to determine if there are any new SMS requirements. The SSM output will indicate the need for an SRM document. If one is required, an SRM panel performs a Preliminary Hazard Analysis (PHA)–type assessment to determine if the NAS would be exposed to any unacceptable risk due to the disposal activity. This may include deactivation, deactivation with a replacement system, or similar considerations.

17. The following would seem intuitive: (1) Once a NAS asset is removed from service, it is no longer a part of the flight day decision-making process. (2) Even if it remains in an operational area in a deactivated state, removal and disposal may occur without regard to aircraft movement. However, SRM is a data-driven (and not intuition-driven) process that still must be conducted.

6.3 Managing Software Risk

6.3.1 Software SRM

Analyzing hazards that are initiated by software, or where software is one of several contributing factors, is different from analyzing hazards that can be caused by hardware that fails or wears out in use. Some of the unique characteristics of software include:

- Software Development Lifecycle (SDLC) – Software follows a defined lifecycle resulting in robust outcomes. Successive steps of architecture, design, coding, development (changes), Quality Assurance / testing (including logic, flow, load, stress, automation, regression, and union), demonstration (user acceptance), release (with configuration freeze), and hot fixes eventually reach an acceptable failure ratio. It is with after-the-fact enhancements and backtracking that field failures often arise.
- Software does not wear out. When software fails, it may be due to a design or implementation defect that has always existed (i.e., a latent defect), a recent enhancement not subject to the full SDLC, or a change in the operating environment that the software was not designed to accommodate.
- Software usually fails without warning. Robust software includes error detection and correction functions to find and fix typical problems using “restores,” “restarts,” and optimization tools. Abnormal error conditions, unexpected process terminations, and long-duration problems not encountered during testing may still arise. Latent defects, specification errors, and issues with enhancements may have existed before the release of the product and may only be triggered or recognized once many software modules are in broad use under a stressing variety of field operating conditions.
- Software can be more complex than hardware. It is common for device software to be hundreds of thousands or millions of lines of code long. Reuse of existing code modules helps reduce errors. Device software may also be integrated with COTS systems software, such as operating systems that can easily reach similar sizes.
- It is difficult to test all of the software in a device and nearly impossible to test all combinations of inputs and branching. Object-Oriented Design helps isolate code into independent blocks with limited process input/output options for ease of development.
- Software is easily changed. Attempts to make last-minute corrections or enhancements can lead to undesired results if the new code does not go through the full SDLC process.

Seemingly insignificant changes in one area of software functionality can lead to defects in unrelated areas of functionality.

6.3.2 Software Development Assurance

RTCA DO-278A establishes an approval liaison process that has similarities to the RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, certification liaison process for aircraft software. However, there are also fundamental differences to be considered. In the case of the aircraft, the applicant is external to the FAA and is regulated by the certification authority. In the case of CNS/ATM systems, the applicant is internal to the FAA, while the software developers are external to the FAA. If it is determined through the safety analyses that the CNS/ATM software can affect systems on board the aircraft, then the assigned Development Assurance Level (DAL) must be acceptable to the aircraft certification authority. The certification authority must also be allowed to provide input to the approval process.

6.3.2.1 Determining the DAL

For software, risk assessment is performed to assign the proper level of rigor to be applied during the software design, development, and testing. An appropriate level of rigor is necessary to ensure confidence that the software does not cause or contribute to a system hazard. Determining the software DAL related to a hazard is a three step process:

1. Determine a hazard's severity classification. A hazard's severity is based on the expected effect(s) of the hazard. Severity is classified according to the severity classifications defined in the ATO SMS Manual.[18]
2. Assign the DAL in accordance with the severity classification. A DAL for software should be assigned according to the severity of the hazard to which the software contributes.
3. Determine if architectural considerations warrant a level different from the initial level. In some cases, architectural mitigation may justify a revision of the DAL to a less stringent classification. Guidance for software architectural mitigation can be found in RTCA DO-278A.

Software that can be a causal factor for hazards must be evaluated to determine the appropriate software assurance level per RTCA DO-278A. Additionally, software design safety requirements, as well as development and testing processes, must be at an assurance level proportional to the degree to which the software product can contribute to a system hazard.

ATO-SG-14-01 provides more detail on determining the correct DAL.

6.3.2.2 Gap Analysis

Many of the non-airborne CNS/ATM systems have been developed and fielded using software development processes other than RTCA DO-278A, such as Institute of Electrical and Electronic Engineers Standard 12207, *Standard for Information Technology – Software Lifecycle Processes*, or vendor's best practices. This creates a potential problem when incorporating RTCA DO-278A software assurance requirements for additions to and/or modifications of these non–RTCA DO-278A legacy systems. For these cases, an RTCA DO-278A Gap Analysis is used to evaluate how the non–RTCA DO-278A processes adhere to the intent of RTCA DO-278A.

An RTCA DO-278A Gap Analysis should be conducted for each function within the system/software being evaluated. RTCA DO-178C/DO-278A guidelines ensure a specific software design and development assurance from the systems safety assessment process, one that is based on software architecture and functions. The RTCA DO-278A Gap Analysis provides a basis for addressing any shortfalls from the required RTCA DO-278A objectives. The gap analysis must be provided to the approval authority[19] and included as an attachment to the Plan for Software Aspects of Approval (PSAA).[20]

It should be noted that conducting the RTCA DO-278A Gap Analysis is not a specific responsibility of the PST. Typically, this effort is led by the PMO acquiring the new system or

18. Note that the severity tables in the ATO SMS Manual are not absolutes; they are simply guides.

19. The approval authority is the ATO authority that accepts and/or approves software lifecycle data for the ground system. This is usually the same office that approves the related safety analyses. For CNS/ATM systems that affect the NAS, this is the ATO Chief Safety Engineer.

20. The PSAA is the primary means used by the approval authority for determining whether an applicant is proposing a software lifecycle that is commensurate with the rigor required for the assurance level of software being developed.

proposing changes to an existing system, with help from the prime contractor conducting systems integration and the subcontractor(s) responsible for developing the software. Other key participants in the process are the RTCA DO-278A SME (someone who has qualified skills and knowledge related to software assurance, specifically related to RTCA DO-278A or RTCA DO-178C) and the Approval Authority.

ATO-SG-14-03 provides more detail on developing an RTCA DO-278A Gap Analysis.

6.3.2.3 Software Approval Process

The software approval authority may review the software lifecycle processes and associated data at his or her discretion to confirm that a software product complies with the approval basis and the objectives of RTCA DO-278A. The software review process assists both the approval authority and the applicant in determining if a project meets the approval basis and RTCA DO-278A objectives. The software review process does this by providing:

- Timely technical interpretation of the approval basis, RTCA DO-278A objectives, approval authority policy, issue papers, and other applicable approval requirements;
- Visibility into the methodologies being used to comply with the requirements and supporting data;
- Objective evidence that the software project adheres to its approved software plans and procedures; and
- The opportunity for the approval authority to monitor SME activities.

The following types of software lifecycle data are related to the approval process:

- PSAA
- Software Requirements Data
- Design Description
- Source Code
- Executable Code
- Software Configuration Index
- Software Accomplishment Summary

ATO-SG-14-02 provides more detail on assessing the software approval process.

6.4 Site Implementation

ATO Order JO 6000.50 complements existing policies regarding SRM and standardizes processes for Operational Risk Management (ORM) during installation activities. ATO Order JO 6000.15, *General Maintenance Handbook for National Airspace System (NAS) Facilities*, defines ORM and clarifies both SRM and ORM policy to assist field managers with risk management activities during installation actions. ORM/SRM integration addresses three distinct categories of effort:

- Implementation Activities,
- Modifications, and
- Required Maintenance.

ATO Order JO 6000.50 also requires that the program office prepares a Generic Site Implementation Plan (GSIP) and conducts SRM on the GSIP itself. A GSIP is required for all

construction, installation, and/or removal activities in the NAS. The GSIP contains an SRM section that provides installers and maintainers with any identified hazards, mitigations, and residual risks identified during the acquisition process, as documented in the System Safety Assessment Report as applicable.

Note that operational risks may have no impact on safety, but must be considered before a system is deployed.

6.5 Legacy Systems SRM

Often, acquisitions support changes to legacy systems. These changes can either result in systems that are functionally identical to the original system or systems that can add to or improve existing functionality. In all cases, the change must be assessed to determine if it introduces/reveals any hazards or affect the safety risk level of the operation/system.

Changes to legacy systems that are initiated due to component obsolescence can be designated as a Technical Refresh. These types of changes include Service Life Extension Programs, Replacement-in-Kind programs, Facility Initiative programs,[21] and Variable Quantity programs.[22] It has been commonly accepted that a change that results in a "box-for-box" replacement of obsolete or unserviceable components containing the identical functionality (i.e., a form, fit, and function replacement) has no impact on NAS safety. However, lessons learned have shown that new hazards may be introduced if a more technically sophisticated multi-component system attribute "box" is being installed to replace a "box" that achieves the same function. If this is the case, then the full SRM process must be followed. If the change does not introduce/reveal any hazards or affect the existing safety risk level of the operation/system, then this may also be documented in an SRM document. The supporting documentation must justify this decision. Refer to the ATO SMS Manual for SRM document requirements.

Changes to legacy systems can include additional functionality or a combination of existing functionality in a way that is not present in the legacy system. New technologies may also have an effect on existing hazards or how they are controlled. For example, a particular function may be enabled by a mechanical switch in the legacy system, but is enabled by software in the Technical Refresh. If the assessment determines that there is new or combined functionality, or if there is any impact to the existing hazards or how they are controlled (including the introduction of any new hazards), then the standard SRM activities documented in the ATO SMS Manual are required.

The conduct of these assessments may be facilitated by examination of the legacy program's ConOps, Functional Analysis, shortfall analysis, EA products, and preliminary requirements in the pPRD, if any exist. Most likely, detailed design and "as-built" technical baseline documentation with successive modifications are sufficient for lifecycle support, yet they may lack in early explanations of the concepts, alternatives, and requirements the legacy system traded-off years ago. Years of live operational data archives may be present, which must be valued more highly than plans, models, or future expectations of performance. For example, many years of adequate specification performance to a frozen baseline at multiple sites

21. A Facility Initiative Program is a program associated with the new construction, replacement, modernization, repair, remediation, lease, or disposal of FAA's manned and unmanned facility infrastructure(s).

22. A Variable Quantity Program is a program that includes insertions, modernizations, or additions to quantities of systems or subcomponents previously fielded and in operation within the FAA.

(actuals) must trump independent, discontinuous future estimates of failure likelihood that ignore such a strong basis for trend analysis. In all cases, the PST should hold an SSM (and consult with the ATO Chief Safety Engineer, as necessary) to determine if the program should develop an SRM document per the current AMS milestone requirements.

A program undergoing a Technical Refresh needs to comply with all aspects of the AMS and SRM processes. The requirements for each Technical Refresh are typically very streamlined or tailored when compared to the original program. For Technical Refresh programs, the PST conducts an SSM (consulting with the ATO Chief Safety Engineer, as necessary) to identify the SRM requirements as soon as practicable. Each Technical Refresh varies in its purpose and requirements, but the SRM requirements may be minimal if the Technical Refresh's form, fit, and function are the same as when the program first went through the AMS.

6.6 Physical Security, Information Security, Cybersecurity, and Occupational Safety and Health

Physical security, information security, cybersecurity, and occupational safety and health issues are only considered within the scope of the SMS if they have safety effects on the operational NAS. This is not to suggest that security- and occupational safety and health−related hazards cannot be dealt with by the appropriate authority; rather, the risk(s) associated with issues such as occupational safety, information security, operational security, physical security, cybersecurity, and Security Certification and Authorization Packages must be transferred to the appropriate authority. In most security cases, this is the FAA System Operations Security Office. For occupational safety and health hazards (including fire and life safety), Environmental and Occupational Safety and Health (EOSH) Services is the appropriate authority for the transfer of risk.

Examples of security hazards such as spoofing, jamming, intentional misuse, or malicious actions would need to be transferred to the appropriate authority, even though they may be considered outside the scope of the SMS. If a safety assessment reveals security or occupational safety and health hazards, those hazards must be documented and transferred to the appropriate authority.

6.7 COTS Products

Using a COTS product, even if it has very high reliability, does not imply that the product is safe when it interacts with other system components. The problem is exacerbated with software because software usually controls many, if not all, of the interactions between system components. Techniques for dealing with COTS by simply equating software reliability or correctness (consistency with specifications) with safety may not prevent system accidents. In many cases, using COTS components in safety-critical systems with acceptable risk may simply be infeasible. In these cases, it is less expensive and safer to provide special-purpose software; using COTS amounts to false economy that costs more in the end.

There are, however, situations in which COTS components can be assured to have adequate system safety. In these cases, either the system design must allow protection against any possible hazardous software behavior or a complete "black box" behavior specification must be provided by the producer of that component in order to perform a hazard analysis.

6.8 Program Risk Management

Program risk management is applied throughout the lifecycle management process to identify and mitigate risks associated with achieving FAA goals and objectives. Each investment

program should institute risk management processes in accordance with AMS policy and guidance. The FAA's policy related to risk management is found in Section 4.13 of the AMS.

Program risk management and SRM have separate foci. For instance, cost and schedule impacts are not factored into a safety assessment, but are a part of program risk management. However, program risk management and SRM are not mutually exclusive. Safety risk that is not properly mitigated can become a program risk by affecting program cost or schedule by delaying or stopping implementing activities. Knowledge of SMS policies and proper planning helps the PM and PST to minimize any SRM impacts to cost and schedule. The AJI SCLs can also assist in this area.

7 Equivalent Processes

Every program is different in scope, complexity, criticality, and resources. In recognition of these differences, programs may use other equivalent processes when conducting the hazard analysis portion of SRM. While these processes may be used, the minimum requirements set forth in the SRMGSA must still be met. An equivalent safety analysis may be used under the following conditions:

- The equivalent process must meet the minimum requirements for the safety analysis outlined in the SRMGSA.
- The use of equivalent processes must be discussed with and approved by the ATO Chief Safety Engineer and documented at the SSM.
- The equivalent process must be described in an approved PSP.

8 SRM Documentation, Approvals, and Tracking

8.1 Safety Risk Management Documents[23]

For an acquisition, the system safety process is a series of analyses that starts at the OSA and the CSA, and continues through the PHA, the SSHA, the SHA, and the Operating & Support Hazard Analysis (O&SHA). Each analysis gets more discrete as more design details are known. The basis of each analysis is a Hazard Analysis Worksheet (HAW). The HAW, initially developed early in the system lifecycle (i.e., in a PHA), is further developed, modified, and enhanced as subsequent analyses are conducted. Each subsequent analysis has a slightly different focus but is essentially a HAW in nature that builds on a previously developed HAW.

Thus, the SRM document becomes a report, or a series of reports, that describe the SRM process that has been conducted with regard to a proposed change or investment. The SRM document records the safety risk analyses that were performed and the findings that support whether the proposed change or investment is free of unacceptable risk. It is a compilation of the SRM documentation completed to date. As such, the SRM document expands with each assessment or analysis as a product moves through the AMS lifecycle. When it is determined at the SSM that specific safety analyses are required, the analyses are documented and become part of the SRM document. Each PST must maintain an SRM document as a record of the progress of the product

In colloquial terms, imagine a folder titled “SRM document for Acquisition XXX”. Every analysis performed for this acquisition is titled “SRM document-(analysis name here)” and stored in the folder. Each analysis is an SRM document but the entire folder is the SRM document for the acquisition. In conversation, especially when a milestone is approaching, you most likely will be asked about the status of “the SRM document”; in most cases, the requestor is really concerned about the status of the particular analysis most recently conducted rather than the entire folder.

In all cases, SRM document activity and information must be recorded in the SMTS.

If an acquisition change is not expected to introduce safety risk into the NAS, there is no need to conduct further safety analysis; however, the PMO/PST must document this determination, along with the justification as to why the change is not subject to additional SRM assessments, in an SRM document. The SRM document must also include a description of the NAS change and affected hardware; software; and/or operational NAS equipment, operations, and/or procedures. The SRM document must also include a justification for the determination that there are no hazards, or any expected change to the current risk associated with the implementation of the NAS change.

8.2 Non-NAS Programs

When an acquisition has an effect on the safety of the NAS, SRM must be conducted and documented throughout the lifecycle of the product or service, in accordance with the SMS. In the AMS, AJI is designated as the responsible office for determining whether an acquisition affects the safety of the NAS. If AJI has determined there is no safety effect, then the ATO Chief Safety Engineer provides documented notification to the JRC Secretariat accordingly. Programs should contact the AJI Safety Engineering Team Manager to initiate discussions if they believe they are exempt from SMS requirements.

23. Risk acceptance must be obtained for any safety analyses in which safety risk is identified, except for the OSA and CSA.

8.3 Peer Review Process

A peer review of SRM documentation determines if it meets SMS policy guidelines and the FAA's safety objectives. A peer review provides for an independent assessment of the documented analysis by multiple people with varying knowledge and experience. This helps ensure that the analysis is technically accurate and makes operational sense (i.e., the safety hazards, causes, effects, and mitigations are appropriate).

All acquisition-related SRM documentation, including PSPs, must undergo a peer review before being submitted to the ATO Chief Safety Engineer for approval. The SRM document is submitted to the AJI-314 Team Manager who assigns an AJI SCL to coordinate the peer review process. The AJI SCL must first review the SRM documentation to determine if it meets all applicable SRM requirements and guidelines of the ATO SMS Manual and the SRMGSA. However, if the SRM documentation is being submitted through the AJI SCL, this step may have already occurred. If the AJI SCL determines that the SRM documentation is not ready for a peer review, it is returned to the originator with recommendations for resolution.

The AJI SCL distributes the SRM documentation for peer review and comments according to the guidelines in the SRMGSA and internal AJI operating procedures. After comments are received and collated, the AJI SCL then works with the PST to generate written responses to originating commenters. The AJI SCL then determines acceptance from the originating commenters, recording any discrepancies associated with partial acceptance or non-concurs. Acceptance can be determined by a combination of e-mail, phone conversations, and meetings. Meetings are preferable when comments and/or responses are complex. A final compilation of all comments and their dispositions is provided to all reviewers.

Figure 8.1 shows a high-level flow diagram of the entire document review process, of which the peer review process is a subset.

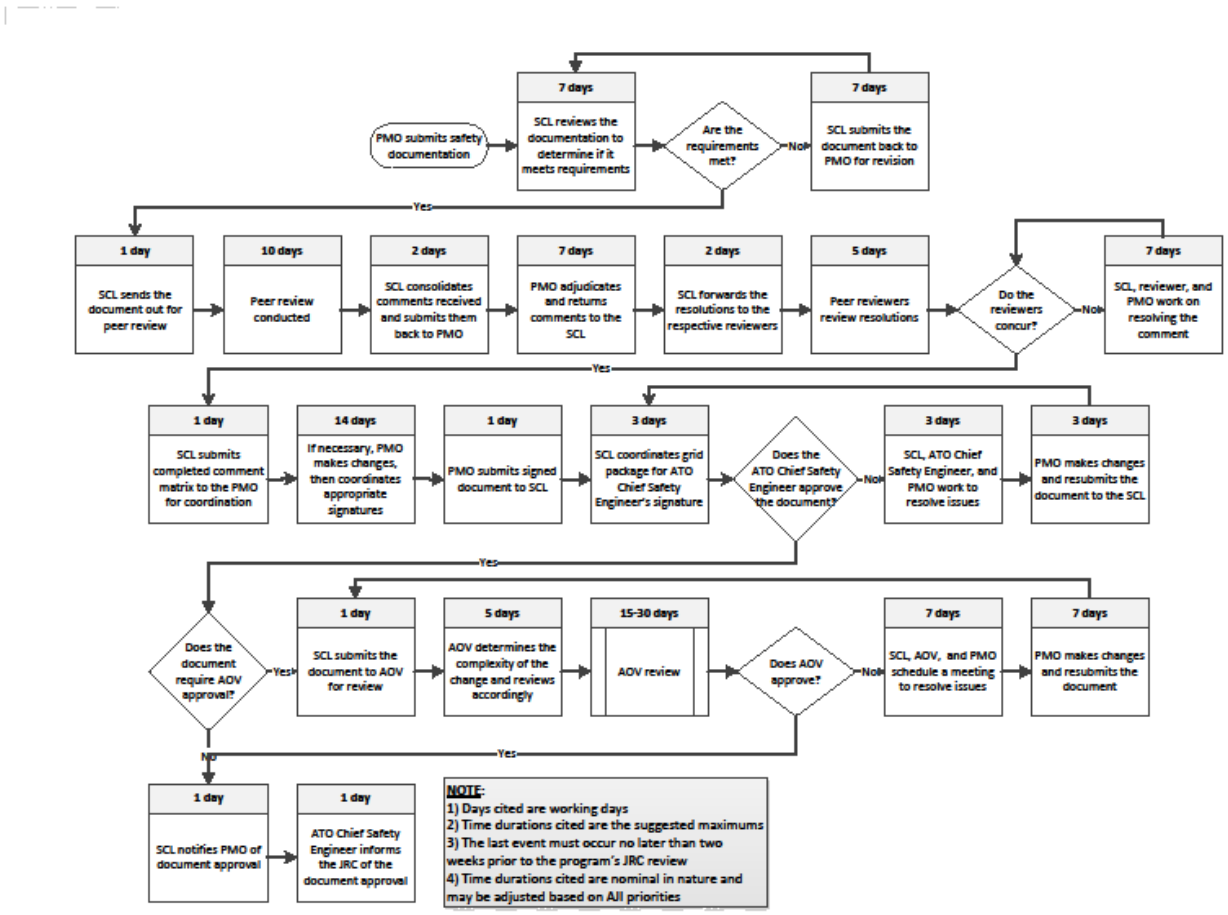

Figure 8.1: Document Review Process Flow

Peer reviewers are designated as either primary or secondary reviewers depending on their role in the approval process, and by the following guidelines:

Primary reviewers include:

- Other AJI SCLs,
- Safety Services representatives,
- ISA Team representatives (IOA-designated programs only),
- ANG Enterprise Safety and Information Security Services Division representatives,
- Representatives from offices responsible for implementing safety requirements (e.g., Aircraft Certification), and
- Representatives from offices responsible for accepting safety risk.

Secondary reviewers as required are:

- Quality Control Group representatives from the Service Center,
- AOV Safety Management Oversight Division representatives,
- Human Factors representatives,
- EOSH Services representatives,
- Cybersecurity representatives, and
- Representatives from other AJI offices.

The peer review timeline is dependent upon various factors including, but not limited to, the complexity of the safety analysis, the number of stakeholders involved, new technologies involved, prior reviews, and projected JRC decision dates. The SCL negotiates with the PMO for firm review dates, if possible, during the initial SSM. Timelines can be reduced if draft versions have been already reviewed. If comments cannot be resolved to the satisfaction of the original commenter, then they are identified as issues for inclusion in the final briefing package provided to the ATO Chief Safety Engineer upon recommendation for approval by the AJI-314 Team Manager.

8.4 Approval Authorities and Coordination Requirements

The ATO SMS Manual contains the guidance and coordination requirements for the review, approval, and risk acceptance of SRM documentation contained completely within a Service Unit, across multiple Service Units, or across multiple LOBs. SRM documentation may not be submitted to the ATO Chief Safety Engineer for approval until after it has gone through the peer review process, as discussed in Section 8.3. The ATO Chief Safety Engineer is also the approval authority for PSPs, as well as the representative that informs the JRC and ISD Secretariats' groups as to which programs are compliant with SMS requirements.

SRM document signature requirements are provided in the ATO SMS Manual, Sections 5.4.3 and 6.0.

8.5 Safety Management Tracking System

AJI has developed the SMTS to track all SRM efforts and approvals from project initiation to the completion of the monitoring plan. The use of the SMTS is required for all safety assessments and analyses, beginning with the OSA and continuing throughout the product's lifecycle. Its primary purpose is to track hazards and their mitigations. The SMTS houses SRM documents, and their associated safety analyses, allowing change proponents and SRM panels to use this information for similar efforts. Additionally, the SMTS tracks the implementation and ongoing monitoring activities, which enables change proponents to assess and track predicted residual risk.

9 Safety Requirements in the AMS Lifecycle

The FAA executes its acquisition management policy using the Lifecycle Management Process, which is organized into the series of phases and decision points shown in Figure 9.1 and described in Section 9.1.

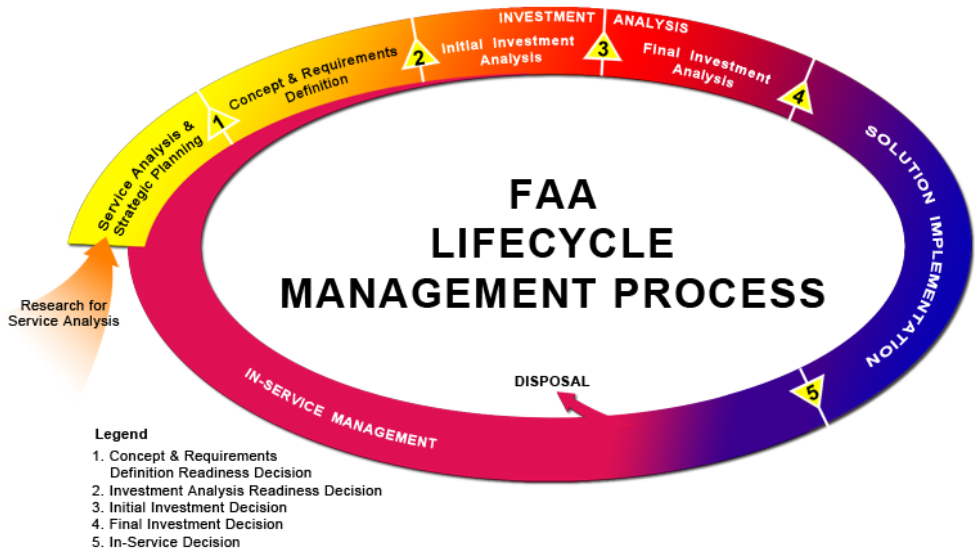

Figure 9.1: FAA Lifecycle Management Process

9.1 The FAA Lifecycle Management Process

The integration of SRM into the AMS process is a major objective of the ATO's SMS. This objective can be achieved by accomplishing SRM tasks using the correct systems safety tools and techniques at the appropriate time to support the decisions made in the lifecycle phase. These tasks are mainly performed by the PMO and result in products packaged in SRM documents, which are reviewed and approved prior to a JRC or ISD.

The circular representation in Figure 9.1 conveys the principles of seamless management and continuous improvement in service delivery over time. Application of the process is flexible and may be tailored appropriately. The AMS policy contains detailed information on the Lifecycle Management Process.

The basis for analyzing and assessing a system differs for each organization. The level at which SRM is conducted also varies by organization, proponent, and the type of change. SRM is carried out at the national level for major system acquisitions. It may be performed at the regional or local level to address proposed changes to equipment or ATC procedures.

Table 9.1 shows when and by whom the various ATO SMS-related tasks should be completed. Appendix B provides further details of the specific program safety requirements by acquisition phase.

Table 9.1: ATO System Safety Analysis Decision Chart

Acquisition Phase	AMS Decision Point	Type of Analysis Required	Documentation Needed	Responsibility for Preparation
Concepts and Requirements Definition	Investment Analysis Readiness Decision	Operational Safety Assessment (OSA) (See Appendix C for guidance)	– SRM document: OSA – Preliminary Program Requirements Document – Enterprise Architecture Safety Plan – Investment Analysis Plan	ANG / PMO
Initial Investment Analysis	Initial Investment Decision	Comparative Safety Assessment (CSA) (See Appendix D for guidance)	– Update to existing SRM document: o CSA – Program Safety Plan (PSP) (See Appendix A for guidance) – Business Case Analysis Report – Briefing to the Joint Resources Council – Initial Implementation Strategy and Planning Document (ISPD) – Preliminary Test and Evaluation Master Plan (pTEMP) – Program Management Plan (PMP)	PMO
Final Investment Analysis	Final Investment Decision	Preliminary Hazard Analysis (PHA) (See Appendix E for guidance)	– Update to existing SRM document: o PHA – Update to existing PSP – Final Program Requirements Document – Final ISPD – Initial TEMP (iTEMP) – Update to PMP	PMO
Solution Implementation	In-Service Decision	Sub-System Hazard Analysis (SSHA); System Hazard Analysis (SHA); Operating & Support Hazard Analysis (O&SHA) (See Appendices F, G, or H for guidance); and Independent Operational Assessment (IOA)	– Final Temp (fTemp) – Updates to existing SRM document: o SSHA o SHA o O&SHA o System Safety Assessment Report (includes Safety Requirements Verification Table) (See Appendix I for guidance) – Update to existing PSP – In-Service Review Checklist	PMO / AJI (IOA only)
In-Service Management	Post-Implementation Review	Review SRM document monitoring plan; Post-Implementation Safety Assessment	– Post-Implementation Review Report	PMO

Appendix A
Guidance for Preparing and Implementing Program Safety Plans

Guidance for Preparing and Implementing Program Safety Plans

1 Purpose

This guidance gives a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for preparing and implementing Program Safety Plans (PSPs) for systems that may be fielded in the National Airspace System (NAS) and that are acquired under the Federal Aviation Administration (FAA) Acquisition Management System (AMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in FAA orders. It reflects updates to the ATO SMS Manual and the Safety Risk Management Guidance for System Acquisitions (SRMGSA), both of which provide guidance on fulfilling requirements set forth in ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*, and the FAA AMS.

3 Background

A PSP is the government's integrated management plan for conducting the system safety program for a particular project or program. By executing this plan, the government ensures compliance with the provisions of the ATO SMS Manual, the SRMGSA, and the AMS. Use of a PSP also ensures that an acceptable level of safety consistent with mission requirements is designed into the system.

Under the leadership of a Program Manager (PM),[1] the Program Safety Team (PST)[2] must develop and tailor a PSP that details the specific safety needs and Safety Risk Management (SRM) requirements of the program and update the PSP as the program matures and information changes. This PSP forms the basis of the prime contractor's corresponding Systems Safety Program Plan (SSPP), which is typically contractually required as a deliverable. The prime contractor's SSPP, when approved by the government, binds the contractor to a system safety program that must be consistent with the government's PSP.

The PSP also stands as the PM's agreement with Safety and Technical Training (AJI)[3] to conduct a safety program that is consistent and compliant with the ATO SMS. It defines the roles and responsibilities of the PM / Safety Team members as they implement the system safety program. As such, the PSP must describe:

- The safety program that applies to each project, subsystem, and interface to support program activities and SMS/SRM requirements;
- The SMS/SRM responsibilities of the PM / Safety Team; and
- Planned SRM efforts.

1. As a program moves through the AMS lifecycle (i.e., from Concept and Requirements Definition (CRD) to the Investment Analysis phase through the Solution Implementation phase and ultimately into In-Service Management), program management responsibilities transfer from the Assistant Administrator for the Office of NextGen (ANG) to Mission Support Services / Program Management Organization / Technical Operations Services.

2. The roles of the PST are defined in the SRMGSA. As with program management, the leadership and composition of these teams may change as a program proceeds through the AMS lifecycle.

3. Or more specifically, with the ATO Chief Safety Engineer, as explained in the SRMGSA.

4 Procedures

There are seven key steps in preparing/implementing a PSP:

- Identify the system safety program requirements;
- Develop a safety strategy based on these requirements;
- Translate the developed safety strategy into a PSP;
- Submit the PSP for approval and signature;
- Implement the system safety program in accordance with the PSP;
- Update the PSP, as needed; and
- Monitor and review the progress of PSP implementation.

4.1 Identify the System Safety Program Requirements

Requirements identification is an initial step that must be conducted in order to tailor a program's safety strategy. The PM, the Safety Team, the AJI Safety Case Lead (SCL),[4] ANG, and other stakeholders collaborate to identify the requirements and solidify them via one or more Safety Strategy Meetings (SSMs). The identification process consists of several sub-steps.

4.1.1 Review Generic Systems Safety / SMS and AMS Program Requirements

The PM / Safety Team should review generic source documentation such as the AMS (specifically Section 4.12), the ATO SMS Manual, the SRMGSA, and applicable ATO and FAA orders (such as ATO Order JO 1000.37 and FAA Order 8040.4, *Safety Risk Management Policy*). This needs to be done to determine the prescribed safety requirements the program must meet at each acquisition milestone.

4.1.2 Review and Accept Pre-decisional NAS Changes Safety Input

The Safety Collaboration Team (SCT) was appointed by the FAA SMS Committee to facilitate the Integrated Safety Management of pre-decisional NAS changes affecting the FAA. In doing so, the committee recognized the need to ensure that safety is not compromised when the FAA proposes pre-decisional changes that affect NAS operations. If the impact of a pre-decisional NAS change crosses Lines of Business (LOBs), Integrated Safety Management must be conducted in accordance with the current FAA Order 8040.4. The SCT's workload is scoped to the SRM of pre-decisional NAS changes, specifically when the impact of the change crosses FAA LOBs. The SCT facilitates teams that conduct Integrated Safety Management on selected pre-decisional changes in accordance with the current FAA Order 8040.4. This could include the facilitation of safety assessments, which may be used as preliminary input data for the safety risk analysis of new system acquisitions or operational changes.

The PM / Safety Team and AJI SCLs must ensure that these results are accepted and translated as applicable into specific program requirements. This must be included as part of the overall program safety strategy. The PM / Safety Team and AJI SCLs must also be able to trace their specific safety requirements back to the portfolio level.

4.1.3 Identify Mechanism for Tacking and Monitoring Program Hazards

ATO Order JO 1000.37 requires that all identified safety hazards and their safety risks be recorded in a database. The PM / Safety Team must use the Safety Management Tracking System to enter data for new safety analyses before beginning the monitoring process. Enter

4. An AJI SCL is assigned by AJI to assist acquisition programs in meeting applicable SRM requirements. His or her roles and responsibilities are delineated in the SRMGSA.

all hazards into the safety management tracking system, including those with low risk. The PM / Safety Team must ensure that personnel have been trained to use this system and that safety management tracking system use is integrated into the system safety program.

4.1.4 Identify Developmental Assurance Requirements

Development assurance is required for systems containing software whose anomalous behavior can cause or contribute to a failure condition with safety-related consequences. Software is a hazard cause and may or may not be a significant contributor to the hazard under consideration. It is highly recommended that development assurance be conducted in accordance with RTCA DO-278A, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*.[5] Since the assurance level can have a significant impact on development costs, it is important to accurately evaluate the software's contribution to a hazard. The methodologies used for this evaluation should be included in the PSP.

4.1.5 Identify Initial Operating Capability Safety Requirements

First-site Initial Operating Capability (IOC) occurs when the operational capability is declared ready for conditional or limited use by site personnel (i.e., after the capability is successfully installed and reviewed at the site and site acceptance testing and field familiarization are complete). IOC requires satisfaction of operational requirements, as well as full logistics support and training for technicians and air traffic specialists to be in place. The PSP must include the specific safety requirements that must be achieved for IOC to be declared.

4.1.6 Identify Post-Implementation Review Safety Requirements

A Post-Implementation Review (PIR) is an evaluation tool used to assess results of an investment program against baseline expectations 6 to 24 months after it goes into operational service. Its main objective is to determine if the program is achieving expected performance targets (including those resulting from safety requirements) and meeting the service needs of the customers. The PIR seeks to validate the original program business case. The PIR also seeks to provide lessons learned with regard to the original program business case for application on future business cases. A PIR strategy is developed in the AMS lifecycle during the Final Investment Analysis and must include appropriate safety considerations, which should be incorporated into the PSP.

For acquisition programs, monitoring responsibilities end when all activities outlined in the Safety Risk Management document monitoring plan and the safety section of the PIR Plan are complete. After the In-Service Decision (ISD), additional safety requirements may be identified via an operational assessment, a PIR, or other means that could result in design changes to the system.

4.1.7 Develop a Nominal Safety Program Schedule

Given that there must be an approved PSP in place at each major Joint Resources Council (JRC) decision point after the CRD phase (i.e., Investment Analysis Readiness Decision, Initial Investment Decision, and Final Investment Decision (FID)) and at the ISD, the PM / Safety Team must develop a nominal safety program schedule consistent with JRC decision points. In addition to JRC decision points, key AMS milestones after FID, including opportunities to verify the incorporation of design safety requirements by inspection (design reviews/audits), by test

5. Other acceptable alternatives exist and can be used with approval from the ATO Chief Safety Engineer.

(DT&E) and by performance (OT&E, IOT&E), should be aligned with the contract schedule. The schedule must also include a requirement for a safety review prior to IOC being declared.

4.2 Develop a Safety Strategy Based on Identified Program Requirements

Given the identified program safety requirements (and any sub-requirements at the testable level of design or performance), the PM / Safety Team develops a safety strategy that is tailored to meet the program's needs. This strategy preparation is done at SSMs with the help of the AJI SCL and in consultation with the ATO Chief Safety Engineer, if necessary (particularly if a large amount of document tailoring is under consideration).

4.2.1 Prepare a Safety Strategy Worksheet

To prepare for the SSMs, the PM / Safety Team must first prepare a Safety Strategy Worksheet (SSW). The SSW is available to the AJI SCL. At a minimum, this SSW must contain the following information:

- System/program name and previous program name, if any.
- Short system description.
- System/FAA/external interface(s).
- Interdependencies.
- Changes to legacy systems, if any.
- Name / phone number of key individuals: PM, leader of the Safety Team, AJI SCL, applicable Service Unit Subject Matter Experts (SMEs), and a RTCA DO-278A SME.[6]
- Where the program is in the AMS lifecycle.
- Any plan for combining JRC decision points.
- Whether alternative solutions may be proposed.
- Proposed dates of the JRC investment decisions and IOC / ISD.
- Impact of the system on the NAS, separation, navigation, communications, and aircraft.
- A listing of any safety assessments completed to date and a summary of any significant safety findings including potential safety risk of the system to the NAS.
- Traceability to a NextGen Portfolio, including any requirements allocated from the portfolio.
- Traceability to NAS Enterprise Architecture (EA) elements (e.g., systems, functions, operational activities, information exchanges, data exchanges). This may be provided in the form of previously delivered program-level NAS EA products.
- Traceability to any previously conducted SCT authorized analyses and assessments that impact the program.
- Independent Operational Assessment (IOA) designation, if applicable.

6. An RTCA DO-178 Designated Engineering Representative would be considered a RTCA DO-278A SME.

4.2.2 Organize and Hold the First SSM

The purpose of this meeting is to review the SSW to ensure the PM / Safety Team, the AJI SCL, and other stakeholders:

- Have a common understanding of the program's safety requirements;
- Outline the acquisition SRM documents required;
- Set a schedule for document preparation, the peer review process, coordination with other LOBs as needed, and approval;
- Tailor and streamline the full acquisition process for proposed actions of less than full acquisition, or non-acquisition solutions; and
- Determine and obtain copies of any prior SRM documents, safety analyses, or assessments that may have value in this proposed action (i.e., concept SRM documents turned into investments, portfolio SRM documents broken out into single systems, legacy SRM documents for replacement, reconfiguration, policy change, or other hard-to-classify non-acquisition actions).

The outcome of this meeting is a safety strategy that is mutually agreed upon by the PM / Safety Team, the AJI SCL, and other stakeholders.

4.3 Translate the Safety Strategy into a Plan

The PSP supports the entire range of activities in every phase of the program. The PM / Safety Team must develop the safety strategy that was agreed to into a plan that includes at a minimum the following information:

- Program scope and objectives;
- Program safety organization;
- Program stakeholders;
- Safety program milestones;
- General safety requirements and criteria, including their traceability to NextGen Portfolios;
- Impact of the system on the NAS (as applicable, including separation assurance, navigation, communications, and aircraft safety);
- Hazard analyses to be performed;
- Hazard tracking system processes to be used;
- Potential safety performance metrics, including safety performance indicators, initial baseline values, and residual target values (safety data to be collected, including metrics, baseline values, safety performance indicators, and target values);
- Safety requirements management[7];
- Safety management of changes to program changes (e.g., scope, design, schedule);

7. The purpose of safety requirements management is to ensure that the FAA documents, verifies, and meets the needs of its internal and external stakeholders. Verification and validation of safety requirements must be conducted to ensure the traceability of safety requirements to both the hazards and to NAS capabilities.

- Safety training required;
- RTCA DO-278 applicability / Development Assurance Level considerations
- Safety interfaces with development engineering, support contractors (pre-FID), prime contractors (post-FID), management, and other specialty engineering groups;
- Dependencies on other PSPs; and
- IOA designation, with justification, if applicable.

4.4 Submit the PSP for Approval and Signature

The following steps are required to obtain approval for each iteration of the PSP:

- The leader of the Safety Team prepares, signs, and submits the PSP to the PM for approval.
- If acceptable, the PM signs the PSP and returns the document to the leader of the Safety Team for further coordination, as necessary.
- The PSP is submitted to the AJI SCL for coordination, approval, and signature by the ATO Chief Safety Engineer.

4.5 Implement the System Safety Program in Accordance with the PSP

Once the document is approved, it becomes the PM's responsibility to implement the PSP as agreed upon with the support of the Safety Team. The PM must also coordinate with the prime contractor to ensure that SSPP-defined safety efforts are being implemented and that they support the safety tasks in accordance with PSP. If IOA is designated, the PM plans and schedules special interest government test facilities, based on availability/qualifications for special government witnesses, and/or hand-on participation by safety personnel in safety requirement validation at the factory, key site, IOA sites, or other on-line developmental environments. Hands-on IOA may not take place using live NAS data at operational locations, although provisions for IOA personnel to monitor or witness live NAS operations may be required.

4.6 Update the PSP as Needed

The PSP is a living document that must be updated by the PM / Safety Team as circumstances change (e.g., different acquisition phases, changes to the program structure/management team, program financial profile, program approach). The PSP must be reviewed prior to each AMS investment decision and before IOC or ISD is declared. If agreements made in the original PSP need to be amended, the AJI SCL must resubmit the revised PSP to the ATO Chief Safety Engineer for approval.

4.7 Monitor and Review the Progress of PSP Implementation

The PM must ensure that the PSP is implemented per the schedule agreed upon, subject to revision due to circumstances, and must inform the AJI SCL of any significant deviations from the plan. The PM must ensure status inputs are entered into the SMTS as a tool to enhance AJI monitoring of the safety program. The AJI SCL must also monitor the safety program on a regular basis, particularly as JRC milestones approach and as certain required documentation must be approved.

Appendix B
Specific Program Safety Requirements by Acquisition Phase

Specific Program Safety Requirements by Acquisition Phase

1 Introduction

The Federal Aviation Administration (FAA) executes its acquisition management policy using a lifecycle management process, which is organized into the series of phases and decision points shown in Figure B.1. Further details on each phase may be found at the FAA Acquisition System Toolset (FAST) website.

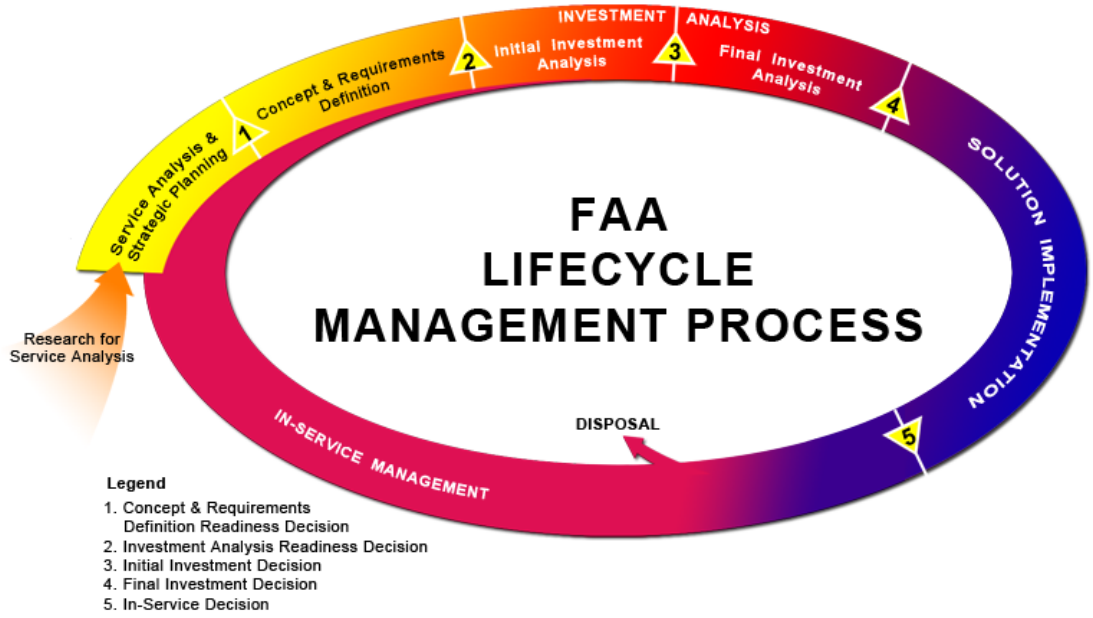

Figure B.1: FAA Lifecycle Management Process

2 Program Safety Requirements for a Concept and Requirements Definition Readiness Decision

2.1 Process Overview

Research and systems analyses are often required during service analysis and strategic planning to mature operational concepts, reduce risk, and/or define requirements before a decision to proceed in the lifecycle management process is made. Service analysis and strategic planning policies apply when determining whether to add a service shortfall or new operational concept to the National Airspace System (NAS) Concept of Operations (ConOps) and FAA Enterprise Architecture (EA).

The Concept and Requirements Definition (CRD) Readiness Decision occurs when an EA roadmap indicates action must be taken to address a critical mission shortfall (often stemming from National Transportation Safety Board recommendations or from emergent In-Service operational issues due to the evolving operational environment, rather than any latent defect of legacy NAS systems). The CRD can also occur to serve some exceptional opportunities that could substantially benefit the FAA. It is based on speculative activities such as simulation, Functional Analysis (FA), and computer-human interface development to define potential requirements, develop operational concepts, and avoid, transfer, or reduce safety risk before entering into Investment Analysis (IA).

2.2 Safety Outputs

The Safety Collaboration Team (SCT) was appointed by the FAA Safety Management System (SMS) Committee to facilitate the Integrated Safety Management of pre-decisional NAS changes affecting the FAA. In doing so, the committee recognized the need to ensure that safety is not compromised when the FAA proposes pre-decisional changes that affect NAS operations. If the impact of a pre-decisional NAS change crosses Lines of Business (LOBs), Integrated Safety Management must be conducted in accordance with the current FAA Order 8040.4, *Safety Risk Management Policy*. The SCT's workload is scoped to the SRM of pre-decisional NAS changes, specifically when the impact of the change crosses FAA LOBs. The SCT facilitates teams that conduct Integrated Safety Management on selected pre-decisional changes in accordance with the current FAA Order 8040.4. This could include the facilitation of safety assessments, the results of which may be used as preliminary input data for the safety risk analysis of new system acquisitions or operational changes.

3 Program Safety Requirements for an Investment Analysis Readiness Decision

3.1 Process Overview

The Investment Analysis Readiness Decision (IARD) occurs at the end of the CRD phase. The IARD determines whether the ConOps, preliminary requirements, EA products and amendments, and preliminary alternatives are sufficiently defined to warrant entry into the IA phase. The decision is made within the context of all ongoing and planned investment activities to sustain and improve service delivery. It ensures proposals are consistent with overall corporate needs and planning.

If the concept under development requires that the proposed system, procedural change, demonstration hardware, or modified software "go live," (in a parallel, online, but nonoperational manner), especially if this involves the NAS for the polling of Air Traffic Control personnel for feedback, suitability demonstrations, field testing, flight tests, or operational prototypes that must be exposed to field conditions only found at operational NAS facilities, then SRM must be conducted. This safety assessment typically uses the Preliminary Hazard Analysis (PHA) worksheet format.

CRD activities occur prior to the establishment of clear functions, baseline requirements, alternative solutions, and solution design.

An Operational Safety Assessment (OSA) may be prepared to provide the system designers and management with a set of safety goals for design. The OSA also provides an operational and environmental description, develops a Preliminary Hazard List (PHL) for the proposal, and assesses the potential severity of the hazards listed in the PHL. In this phase, the results of any early safety analyses or assessments that impact the program are inputs to the OSA. In addition, certain planning must occur prior to the IARD, such as development of an Investment Analysis Plan (IAP) to include relevant safety information.

For replacement, removal, or reconfiguration of existing NAS systems, significant existing design, test, field performance, NAS operations research, and detailed support documentation (perhaps including recent Safety Risk Management documents or portfolio SRM documents) may already exist; these may apply substantially to the new proposed action. Consider an audit for applicable and reusable baseline documents and SRM documents that can form a sound basis for legacy architecture, requirements, design, performance, and known NAS constraints.

3.2 Safety Output

3.2.1 Program Safety Plan

The Program Safety Plan (PSP) is the Program Manager's (PM's) plan for the program's safety process. The PSP is used to ensure compliance with provisions of the Air Traffic Organization (ATO) SMS Manual. The PM must adjust the PSP to the specific needs and SRM requirements of the program consistent with the phase of the AMS lifecycle that the program is entering. The tailoring of the PSP must be in accordance with Safety and Technical Training (AJI) and Service Unit policy and agreements made at the Safety Strategy Meeting (SSM). The ATO Chief Safety Engineer may require programs to identify additional features or text for inclusion.

A PSP must be developed and tailored specifically for each program requesting an IARD. The PSP supports the IARD and is completed and approved prior to the Joint Resources Council (JRC) Secretariat's cut-off date for the IARD. Early in the acquisition lifecycle, the PSP may be very high level, as many of the program specifics are not yet known. The PST further develops the PSP as the acquisition matures. At the IARD, the typical PSP should cover the following:

- Safety program scope and objectives,
- Description of the range of alternatives / alternative systems / generic capability,
- Safety organization,
- Nominal safety program milestones,
- General safety requirements,
- Management of safety program, and
- Interfaces with other programs teams.

See Appendix A for further details on preparing a PSP.

3.2.2 Operational Safety Assessment

The OSA is a tool based on the assessment of hazard severity. The OSA also establishes how safety requirements are to be allocated between air and ground components and how this might influence performance, interoperability, and monitoring. The OSA is completed during the CRD phase and must be approved prior to the JRC Secretariat's cut-off date for the IARD, which is about two weeks before the IARD JRC meeting date.

An OSA provides a disciplined method of objectively assessing the safety requirements of new NAS concepts and systems, typically for Communication, Navigation, and Surveillance and Air Traffic Management systems. The OSA identifies and assesses the hazards in a system, defines safety requirements, and builds a foundation for follow-on institutional safety analyses related to IA, Solution Implementation (SI), In-Service Management (ISM), and Service Life Extension Programs.

OSA-identified severity codes are mapped to a pre-set level of probabilities, which establishes the necessary safety level required for controlling the hazard. This means that a hazard with a catastrophic severity would be mapped to a probability requirement more stringent than would a minor severity hazard. This process establishes the level needed for controlling the hazard at or below a medium-risk level, which assists in establishing safety requirements for the concept or system design.

See Appendix C for further details on preparing an OSA.

3.2.3 Software Development Assurance

Planning for development assurance needs to begin early in the Acquisition Management System (AMS) lifecycle so the Development Assurance Level (DAL), as defined in the Safety Risk Management Guidance for System Acquisitions (SRMGSA), can be factored into the Business Case Analysis. Typically, this occurs prior to the IARD, while the OSA is being developed. The DAL is initially established from the OSA and is included in the preliminary Program Requirements Document (pPRD).

3.2.4 Preliminary Program Requirements Document

Preliminary program requirements specify what the new capability must do and how well it must perform its intended functions. Safety is one of the key disciplines in the AMS and must be addressed. Safety requirements identified in the OSA that are also system requirements must be included as requirements in the pPRD. The PMO must plan for the fulfillment of safety performance requirements by testing. Tagging requirements that are of interest to safety flags them for special oversight.

3.2.5 Investment Analysis Plan

The IAP is a CRD phase requirement. It defines the program's scope, assumptions, alternatives, and organizational roles and responsibilities in IA. The IAP template is available on the FAST website. There is a section of the IAP that contains the requirement for reporting the results of safety assessments in the IAP as it is formulated and updated when the program goes through the AMS process.

4 Program Safety Requirements for the Initial Investment Decision

4.1 Process Overview

The Initial Investment Decision (IID) is the point at which the JRC approves or selects the best alternative that meets the required performance and that offers the greatest value to the FAA and its customers. To support that decision, the Comparative Safety Assessment (CSA) is completed to inform the Program Management Organization (PMO) and JRC of the relative risk ratings of each alternative. At this stage, the initial Program Requirements Document thoroughly defines the program's requirements and maintains requirements traceability against the single preferred alternative chosen at IID. Non-preferred alternative requirements are deleted as a result of the IID and should not be populated in the Safety Management Tracking System. In the AMS, the Portfolio Selection Criteria Guidance for the IID shows the role played by safety and is available on the FAST website.

4.2 Safety Outputs

4.2.1 Program Safety Plan

Prior to receiving an IID decision, the PSP must be updated with the latest information. At this phase of the acquisition lifecycle, there could be changes in the management and PST as the program moves from the Office of NextGen (ANG) to ATO control. Also, the PM must plan to conduct the CSA, an essential analysis needed to receive an IID.

4.2.2 Comparative Safety Assessment

A CSA provides management with a listing of all of the hazards associated with a change, along with a risk assessment for each alternative hazard combination that is considered. Alternatives can affect cost and schedule by requiring different levels of additional safety analyses and requirements to properly address the different risk levels. Therefore, the CSA is used to rank

the options from a safety perspective for decision-making purposes. Other considerations for decision makers, such as cost, schedule, training, and other implications, are not within the scope of a CSA. Those considerations are discussed by the PMO in the IAP cost analysis and in similar Business Case reports.

The CSA is a risk assessment; it defines both severity and likelihood in terms of the initial and predicted residual risk of the solution. The likelihoods determined are for the worst credible outcome occurring. The CSA builds upon the OSA using the top-level FA from the OSA, but typically decomposing it by at least one more level in order to expand upon the PHL produced by the OSA. Each alternative is described in sufficient detail to ensure the audience can understand both the proposed solution and the hazards and risks developed. Per the AMS, alternatives selected and assessed are technical alternatives, not installation or procurement alternatives.

The expanded PHL is developed from the FA, at which point each hazard's risk is assessed in the context of the alternatives. For hazards related to human error, tools that specifically address human performance and reliability rates (including associated performance shaping) may be employed. (See the ATO SMS Manual for additional information.) After this is done, requirements and recommendations can be made based on the data in the CSA. A CSA should be written so that the decision-maker can clearly distinguish the relative safety merit of each alternative.

See Appendix D for further information on preparing a CSA.

4.2.3 Software Development Assurance

The DAL, as defined by the SRMGSA, is validated in the CSA, which may differ between investment alternatives. The DAL for the alternatives is then included in the IAP and Implementation Strategy and Planning Document (ISPD) prior to the IID.

5 Program Safety Requirements for the Final Investment Decision

5.1 Process Overview

Systems safety has a twofold purpose leading up to the Final Investment Decision (FID): to develop early safety requirements that form the foundation of the safety and interest systems engineering efforts and to provide objective safety data to aid acquisition management in their decisions. The early assessment allows for informed, data-driven decisions.

The FID is the point at which the JRC approves the program, sometimes with Record of Decision changes and special direction. To support FID, a PHA is completed to inform the PMO and JRC of the risk ratings for the program. The required work products of the Final IA must be verified and validated (according to the FAA AMS Verification and Validation (V&V) guidance) prior to the FID. If the JRC accepts the recommendations, it approves the investment program for implementation, delegates responsibility to the appropriate service organization, and approves the final Program Requirements Document (fPRD), final business case, and the final ISPD, all of which have safety embedded in them.

5.2 Safety Output

5.2.1 Program Safety Plan

Prior to release of the Screening Information Request for contractor proposals, the PSP must once again be updated and expanded, as it forms the basis of the contractor's corresponding

Systems Safety Program Plan (SSPP), if contractually required. The PSP supports the FID and is completed and approved prior to the JRC Secretariat's cut-off date for the FID.

The contractor's SSPP, when reviewed and approved, shows how and when the vendor or contractor intends to meet the specified PSP requirements. The review and approval authority for the SSPP is the PMO. The SSPP details the following:

- Contractor's program scope
- Safety organization
- Program milestones
- Requirements and criteria
- Hazard analyses
- Safety data
- Verification of safety requirements
- Auditing and monitoring program
- Post-Implementation Review (PIR) plans
- Training
- Accident and incident reporting
- Interfaces

The Data Item Description (DID) for an SSPP (AJI-DID-SSPP-001) outlines the contents to be included in the SSPP.

The typical PSP prior to the FID covers the following:

- Program scope and objectives;
- Safety organization;
- Safety program milestones;
- General safety requirements and criteria;
- Hazard analyses to be performed;
- Hazard tracking system processes to be used;
- Safety data to be collected;
- Safety requirements management, including how to manage the Safety Requirements Verification Table (SRVT);
- Safety assessments and reports for changes to program, design, and engineering;
- Safety training required;
- Safety interfaces with design engineering, contractors, management, and other specialty engineering groups;
- Safety Assessment Review Plan (i.e., the type of safety assessment program to be used and scheduled for accomplishing safety V&V);
- PSP management of cost and schedules; and
- Interfaces with other program and integrated safety plans.

5.2.2 Preliminary Hazard Analysis

The PHA is a common hazard identification and analysis tool used in nearly all SMS applications. Its broad scope is an excellent guide for the identification of issues that may require more detailed hazard identification tools. The PHA focuses on the details of the solution architecture, including the implications for human reliability. In addition to the historical experiences used for the PHL, information about technologies, materials, and architectural features such as redundancy and human-system integration are available as sources of the PHA.

The PHA can be conducted with input from the OSA, CSA, FA, and/or the Bow-tie Model. It is important to note that the OSA and CSA may not have been performed if the ATO Chief Safety Engineer waived the requirement to perform those assessments. Although an FA or a Bow-tie Model is not required, they are both highly recommended, as they can assist in the hazard identification process and subsequent portions of the analysis. A human reliability analysis or assessment (the expansion of the PHL to include risks, hazards, credible effects, and mitigations to manage the risk) may also be conducted.

The PHA is conducted after the alternatives are evaluated and a single alternative is selected as the best option. This means it is conducted after the CSA and before the FID. The PHA subset of the SRM document is completed and approved prior to the JRC Secretariat's cut-off date for the FID. PHAs are usually conducted by the government. However, the DID for a PHA (AJI-DID-PHA-001) outlines the contents to be included in a PHA if conducted by a system developer.

See Appendix E for further information on preparing a PHA.

5.2.3 Final Program Requirements Document

The fPRD contains all new and existing systems safety requirements accepted by the program. The mitigations identified in the SRM document that are allocated to the program may show up as architectural, functional, design, or performance requirements or as Statement of Work tasks with deliverables in the fPRD. These safety items must be uniquely identified and any requirements must be able to be parsed into the SRVT. If all the identified safety requirements in the fPRD are eventually fulfilled and verified, the program is expected to attain its predicted residual risk. If not, the resultant risk rating may be as high as the initial risk rating determined in the PHA.

Changes in the NAS environment in which the new capability is targeted to operate may evolve while solution development takes place. Setting baselines of requirements, design, production, and "as-built" configuration makes fulfillment of new safety needs ever more expensive under this original program segment or capability increment. Future investment segments, increments, options, and contingencies may be recognized to reorganize solution development into phases. Actual residual risk may well be higher or lower depending on the sum total of all outside influences and developments in NAS operations over the years it takes to field the new system.

5.2.4 Implementation Strategy and Planning Document

The ISPD provides the investment decision authority with a summarized characterization of the plans for the SI phase of the proposed investment. It conveys the most critical, relevant, and meaningful information to support JRC decision making. The IID requires an initial ISPD covering specific sections identified in the ISPD template. An FID requires a complete ISPD. After the FID, the ISPD can only be modified if the program returns to the JRC to rebaseline the

investment decision. Rebaselines are discouraged; therefore, the ISPD must provide high-confidence, comprehensive, and contingent plans that fit within the baseline and anticipate all potentialities.

The scope of the safety effort in the ISPD must be well understood and risk must be adjusted for high confidence. Within the ATO, the ISPD is approved by both the Vice President of the organization that executes the program and by the Chief Operating Officer. Certain sections of the ISPD are reviewed and approved by specific executives, including the Vice President of AJI. Final signed approval of the ISPD by all members of the JRC is concurrent with the investment decision. There is a section of the ISPD specific to the SMS. The ISPD template is available on the FAST website.

5.2.5 Test and Evaluation Master Plan

The Test and Evaluation Master Plan (TEMP) is the primary test management document for an acquisition program throughout its lifecycle from Investment Analysis through In-Service Management. It describes the baseline test strategy and the scope of a test program. The TEMP delineates all activities that must be performed to achieve the goals of V&V. It also documents the test and evaluation methodologies that will be used to assess safety hazard controls and security risks. Programs requiring a TEMP will produce a preliminary TEMP for IID, an initial TEMP for FID and a final TEMP during SI.

5.2.6 Program Management Plan

The Program Management Plan (PMP) defines how the service organization manages the investment program to execute the strategy recorded in the ISPD. It defines the relationships and responsibilities of key organizations that contribute to the implementation and fielding of this initiative. All investment programs that have a safety impact on the NAS are required to execute a system safety management program as specified in the PMP.

5.2.7 Software Development Assurance

The final DAL, as defined in the SRMGSA, is determined from the PHA. This final DAL is included in the fPRD and PSP. Any changes to DAL are included in the final versions of the Business Case Analysis and ISPD prior to the FID.

6 Program Safety Requirements for an In-Service Decision

6.1 Process Overview

The In-Service Decision (ISD) authorizes deployment of a solution into the operational environment, and occurs after demonstration of Initial Operating Capability (IOC) at the key site. The ISD establishes the foundation for the declaration of operational readiness at the key site and IOC at subsequent sites. An approved SRM document is required at IOC; it must be updated prior to the ISD to reflect national deployment. Prior to the ISD, all of the safety-related In-Service Review (ISR) checklist items must be closed or have an approved Action Plan. The ATO Chief Safety Engineer must concur with the closure of the ISR checklist items and any related Action Plans. The Director of Policy and Performance approves the Action Plan as the Closing Authority, and he or she concurs with the closure of the Action Plan. Statuses of ISD Action Plans are reported to the ISD Secretariat and tracked to closure.

The full suite of safety analyses required by the ATO and the SSM, all of which are listed in the PSP and SSPP, must be done prior to the ISD. Typical safety assessments, usually performed by the prime vendor or its subcontractor, include those listed in Section 6.2 below.

6.2 Safety Output

6.2.1 Program Safety Plan

Prior to ISD, the PSP must be expanded to include any safety planning required to support the PIR.

6.2.2 Sub-System Hazard Analysis

A Sub-System Hazard Analysis (SSHA) is a safety risk assessment of a system's sub-systems/components conducted by the system developer at a deeper level than is provided in a PHA. In cases where system development is performed by the vendor, the SSHA is typically assigned per the Statement of Work. The SSHA uses the same worksheet as the PHA and is performed early in the lifecycle of a system, providing valued inputs to the development of requirements in the early phases of system development. It is an analysis type that examines each sub-system or component (including the human component); identifies hazards associated with normal and abnormal operations; and is intended to determine how operation, failure of components, or other anomalies might adversely affect the overall safety of the system. It also aids in the further determination of safety risk and the need for additional safety requirements. The output of the SSHA is used to develop systems safety requirements and to assist in preparing performance and design specifications. In addition, the SSHA establishes the framework for the performance of follow-on hazard analyses.

The SSHA is an important part of any systems safety program. It provides detailed analysis that identifies hazards and recommends solutions. The design details are known and the analyses cover all details that are necessary to identify all possible safety risks.

Most SSHAs are documented in the matrix format, though some use fault trees or other forms of logic diagrams. Fault trees alone are incomplete and do not directly provide useful information. The utility of fault trees comes from the cut and path sets they generate, the analysis of the cut and path sets for common cause failures, and the independence of failures/faults. Fault trees are good for analyzing a specific undesired event (e.g., rupture of a pressure tank) and can find sequential and simultaneous failures but are time consuming and expensive.

SSHAs are more detailed than the PHA and are intended to show that the sub-system design meets the safety requirements in the sub-system specifications. If hazards are not identified and corrected during the design process, they might not be identified and corrected later when the sub-system designs are frozen and the cost of making a change is significantly increased.

The DID for an SSHA (AJI-DID-SSHA-001) outlines the contents to be included in the SSHA.

See Appendix F for further information on preparing an SSHA.

6.2.3 System Hazard Analysis

The System Hazard Analysis (SHA) analyzes the whole system and the internal and external system interfaces. Its general purpose is to perform a detailed safety risk assessment of a system's interfaces with other systems and the interfaces between the sub-systems that compose the system being studied.

The SHA is typically conducted by the system developer. In cases when system development is performed by the vendor, the SHA is typically assigned per the Statement of Work. The SHA uses the same worksheet as the PHA, and is performed early in the SI phase of the lifecycle of a system, providing important input to the development of requirements in the early phases of

system development. The SHA aids in the early determination of risk and the need for additional safety requirements for system hazards. The output of the SHA may be used to develop additional systems safety requirements and to assist in preparing performance and design specifications. In addition, the SHA is a basic hazard analysis that establishes the framework for follow-on hazard analyses that may be performed.

The SHA should begin as the system design matures, at the preliminary design review or the facilities concept design review milestone. It should be updated until the design is complete. The SHA is used to identify new requirements and support the V&V of existing requirements.

For the most part, the description of the SSHA also applies to the SHA.

The specific uses of the SHA are to:

- Verify system compliance with safety requirements in the system specification;
- Identify previously unidentified hazards associated with the system interfaces, system functional faults, and system operation in the specified environment;
- Assess the safety risk of the total system design;
- Consider human factors, system/functional failures, and functional relationships between sub-systems comprising the system (including software);
- Identify and verify existing controls;
- Initiate and/or update the SRVT;
- Recommend and validate additional mitigations or controls; and
- Develop processes to control and track hazards.

The DID for an SHA (AJI-DID-SHA-001) outlines the contents to be included in the SHA.

See Appendix G for further information on how to prepare an SHA.

6.2.4 Operating and Support Hazard Analysis

The general purpose of the Operating and Support Hazard Analysis (O&SHA) is to perform a detailed, systematic safety analysis addressing hazards and risk applicable to the operation and the support activities of a given system.

The O&SHA uses the same worksheet as the PHA and identifies hazards and risks occurring during operation of the system. This primarily encompasses the procedural aspects, as well as the support functions (e.g., maintenance, servicing, overhaul, facilities, equipment, and training). Its purpose is to evaluate the effectiveness of controlling procedural hazards instead of only those hazards created by design. Additionally, the O&SHA should ensure that procedures do not introduce new hazards.

The timing of the O&SHA is important. In most cases, procedures are not available for review until the system begins initial use, demonstration, prototype, or initial test and evaluation. As a result, the O&SHA is typically the last formal analysis to be completed, usually mid-way through the SI phase. The sooner the analysis can begin, the better. Even before the system is designed, an O&SHA can begin identifying hazards within the anticipated operation of the system. Ideally, the O&SHA should begin with the formulation of the system and not be

completed until sometime after its initial test (which may identify additional hazards). This is critical; design and construction of support facilities must begin far before the system is ready for fielding, and all special safety features must be identified early on, or the costs to modify the facilities may force PMs and users to accept unnecessary risks.

It is important to ensure that the analysis considers not only the normal operation of the system, but also abnormal, emergency, or degraded operation; system installation; maintenance; servicing; storage; evaluation of training; and other operations. Misuse must also be considered. In other words, if anyone is doing anything with the system, planned or unplanned, the O&SHA should cover it.

The DID for an O&SHA (AJI-DID-O&SHA-001) outlines the contents to be included in the O&SHA.

See Appendix H for further information on how to prepare an O&SHA.

6.2.5 System Safety Assessment Report

The general purpose of a System Safety Assessment Report (SSAR) is to conduct and document a comprehensive evaluation of the safety risk being assumed before the program is deployed into the NAS. This means that the SSAR summarizes the safety analyses and assessments previously conducted on the program. The SSAR is a continuous, closed-loop process containing the SRVT. The SRVT contains all of the safety requirements identified with the origin of the requirement (e.g., OSA, CSA, PHA, SSHA, SHA, and O&SHA), including V&V. At the ISD or IOC, all safety requirements must undergo V&V by the PMO. Objective evidence of V&V closed status may be reviewed by the ATO Chief Safety Engineer upon request.

Per the ATO SMS Manual and the FAA NAS Systems Engineering Manual (SEM), verification is the process that ensures that the product is being built right (according to specifications). Validation is the process of proving that the product being built is operationally suitable and effective. Both verification and validation must be successful to deploy the product.

The report provides an overall assessment of the safety risk associated with the product. It is crucial that this assessment report be developed as an encapsulation of all the analyses performed. For Independent Operational Assessment (IOA)−designated systems, it must be updated to reflect IOA results as appropriate. Safety hazards documented during IOA should be evaluated by the PST to determine if there is impact on prior safety analyses, determine if additional analysis is needed, and then develop appropriate mitigations and monitoring for the IOA safety hazards. The SSAR contains a summary of the analyses performed and their results, the tests conducted and their results, and the compliance assessment. The SSAR must include:

- The safety criteria and methodology used to classify and rank hazards, including any assumptions made from which the criteria and methodologies were derived;
- The results of the analyses, demonstrations, assessments, and testing conducted;
- The hazards that have an identified residual risk and the assessment of that risk;
- The list of hazards and the specific safety recommendations or precautions required to reduce their safety risk; and
- A discussion of the management and engineering decisions affecting the residual risk at a system level.

The final section of the SSAR should be a statement by the PMO describing the overall risk associated with the system and the PMO's acceptance of that risk.

The DID for an SSAR (AJI-DID-SSAR-001) outlines the contents to be included in the SSAR.

See Appendix I for further information on how to prepare an SSAR.

6.2.5.1 How to Use the SSAR

An SSAR must be conducted prior to any ISD or IOC decision point. Conducting the SSAR is an ISR requirement.

The specific uses of the SSAR are to:

- Summarize the results of the program's SRM efforts;
- Identify all safety features of hardware, software, interfaces, and system design;
- Identify hazards related to procedures, human factors, hardware, and software identified in the program to date;
- Update the SRVT to show the V&V status of each safety requirement and the hazards to which those requirements are applied; and
- Assess readiness based on safety risk when proceeding with test or operation.

All hazards must be included in a monitoring plan. This must be approved by the ATO Chief Safety Engineer as part of the SSAR. In the event that the SSAR reveals some requirements not yet verified, the risk may need to be reassessed for accuracy. The PMO submits the results of the SSAR to the ATO Chief Safety Engineer.

As previously mentioned, the status of mitigations are shown in the SRVT. Before IOC, AJI and the PMO work together to determine if the listed safety requirements have been met to a point where IOC can be declared. This is done on a case-by-case basis. After IOC and before an ISD is declared, the PMO may conduct an Operational Suitability Demonstration, and AJI may conduct an Independent Assessment. This may lead to the identification of additional safety requirements, and the SSAR/SRVT may have to be updated.

6.2.5.2 Types of Safety Reviews

The SSAR can be accomplished through one or more safety reviews. The types of safety reviews are:

- **Periodic Review:** These are reviews done throughout the life of a program. They evaluate the status of hazards based on the verification of controls and requirements, and help in monitoring the effectiveness of the controls.

- **Phased Review:** These are reviews conducted for defined portions of the implementation of solutions into the NAS. Phased reviews apply to a single JRC decision, which involves implementing a solution in steps or phases. The program itself does not need to use the term "phased" in its title. As long as the implementation is incremental or in steps, each increment or step has safety reviews. The reviews evaluate the status of hazards based on the verification of mitigating requirements for that particular phase.

- **Final Implementation Review:** These are reviews conducted for a program's ISD and IOC. The reviews evaluate the status of hazards based on the verification of the program's requirements.

6.2.6 Safety Requirements Verification Table

The SRVT is an evolving list of safety requirements that starts with the first safety assessment. Safety requirements are controls written in requirements language and used to control hazards. Changes to safety requirements must be reported to the program office and to the ATO Chief Safety Engineer.

The SRVT contains the following information:

- A list of requirements identified in any safety assessment for a given program (e.g., OSA, CSA, PHA, SHA/SSHA, O&SHA),
- V&V information, and
- The level of risk controlled by the requirement.

6.2.6.1 Using the SRVT

The SRVT is used to accomplish the V&V process for safety requirements. The PMO must assure all safety requirements are captured within the SRVT.

The SRVT is intended to provide a continuing list and status of safety requirements that result from the SRM process. The requirements that are contained in this list must meet the standards detailed in the FAA NAS SEM.

6.2.7 Software Development Assurance

The DAL is established prior to contract award based only on functional requirements. The hazard assessments performed by the developer occur after contract award, which could be some time after the initial establishment of the DAL. It is important to verify that the DAL is appropriate after the hazard assessments are performed and after any change in system requirements.

6.2.8 ISR Checklist

The ISR checklist is specific to systems safety and must be completed in support of the ISD. By reviewing the checklist early in a program's AMS lifecycle, the PMO better understands the steps that must be completed. As programs approach ISD, the AJI Safety Case Lead, on behalf of the PMO, coordinates with the AJI Safety Engineering Team Manager to ensure that the systems safety management portion of the checklist has been completed. The ISR checklist may be downloaded from the ISD page of the FAA employee website.

7 Program Safety Requirements for ISM

7.1 Process Overview

7.1.1 Monitoring Mitigations and Tracking Hazards

See the ATO SMS Manual for detailed guidance on risk monitoring and tracking.

7.1.2 Post-Implementation Review Safety Considerations

A Post-Implementation Review (PIR) is an evaluation tool used to assess the results of an investment program against baseline expectations 6 to 24 months after it goes into operational

service. Its main objective is to assess an investment program, determining if it is achieving expected performance and benefit targets, if it is meeting the service needs of customers, and if the original business case is still valid. The PIR process is governed by Section 4.15.1 of the AMS.

A PIR Strategy is developed during the AMS lifecycle during the Final IA. It identifies sites at which the review will be conducted, when the review is expected to occur, any limitations to the review, products of the review, and participating organizations and their responsibilities. All investment programs are potentially reviewed based upon their assigned acquisition category. SMS considerations for inclusion in the PIR Strategy are discussed during an SSM held with the ATO Chief Safety Engineer, PIR Quality Officer, and the PMO.

A PIR plan[1] is developed prior to ISD during the AMS lifecycle by the PIR Team for the investment program under review. It is a detailed expansion and refinement of the PIR strategy, defining expected outcomes, planned activities, and resources necessary to complete the review. SRM input to the plan should be finalized after the SSAR is completed and approved. The ATO Chief Safety Engineer reviews the safety input to the PIR plan and provides concurrence or recommendations to the PIR Team Leader and PIR Quality Officer.

A PIR report is prepared by the PIR Team[2] after the review is completed. The ATO Chief Safety Engineer reviews the report's safety findings (including safety data that verifies whether the predicted residual risk has been met) and recommendations and provides concurrence or recommendations to the PIR Quality Officer. If the PIR reveals an increased safety risk, the risk acceptor must coordinate a reassessment to determine if changes to the mitigation strategy are necessary. An SRM panel must be convened to assess the risk of any new hazards and/or to develop additional safety requirements to ensure risk is acceptable.

After the PIR report is complete, a plan of action and milestones (with completion dates) is developed to address the report's recommendations. These recommendations support the ISM phase during the AMS lifecycle and are reported to the investment decision authority, Vice President or equivalent, and key stakeholders, including AJI.

See the FAST website for information on how to conduct a PIR and report results, including those specific to SRM. Refer to the ATO SMS Manual for additional details of assessments and evaluation and for additional details.

1. The PIR is organized and managed by the PIR Quality Officer in Acquisition Policy and Oversight / Acquisition and Contracting / Office of Finance and Management.

2. The AJI Safety Case Lead should participate as a member of the PIR Team.

Appendix C

Guidance for Conducting and Documenting an Operational Safety Assessment

Guidance for Conducting and Documenting an Operational Safety Assessment

1 Purpose

This guidance gives a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for conducting and documenting an Operational Safety Assessment (OSA) of solution concepts.

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the system engineering processes referred to are described in the National Airspace System (NAS) System Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS Section 4.12, National Airspace System Safety Management System
- ATO SMS Manual
- ATO Order JO 1000.37
- NAS SEM
- Safety Management Tracking System (SMTS) User Manual
- ATO Safety Guidance (ATO-SG) 14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*

3 Background

3.1 Description

An OSA must be conducted to identify, analyze, and document operational hazards and associated safety requirements early in the AMS Planning Phases. It is an important part of the FAA's acquisition planning process, especially for the Office of NextGen (ANG), the Program Management Organization (PMO),[1] and the Program Safety Team (PST).[2] The OSA provides early identification and documentation of safety requirements that could improve safety and product integration, lower developmental costs, and increase product performance and the probability of program success.

For ANG, an OSA, which may include inputs from Safety Collaboration Team (SCT)–mandated[3] safety analyses or assessments, is an indispensable tool for allocating safety requirements to

1. As a program moves through the AMS lifecycle (i.e., from Concept and Requirements Definition (CRD) to the Investment Analysis phase, through the Solution Implementation phase, and ultimately into In-Service Management), program management responsibilities transfer from ANG to Mission Support Services, the PMO, or Technical Operations Services.
2. A PST is a resource provided by the PMO to support the safety efforts of the acquisition throughout the AMS lifecycle. As with program management, the leadership and composition of the PST changes as a program proceeds through the AMS lifecycle.
3. The SCT serves as the technical advisory body to the FAA SMS Committee. The SCT's primary function is to facilitate the Integrated Safety Management of pre-decisional NAS changes.

lower-level increments.

OSAs are typically conducted by the PMO in-house with assistance from the PST and participation from the necessary stakeholders. Some OSAs are international or industry-wide in scope and may be conducted by industry-wide working groups chaired by external entities (e.g., RTCA, Inc.) acting under the guidance of the FAA.

Unlike follow-on safety assessments, an OSA does not consider overall safety risk; rather, it is used to assess hazard severity and determine the target level of likelihood required to achieve an acceptable level of safety. It may also be used to help develop safety requirements. An OSA is typically conducted during the CRD phase of the AMS lifecycle and is approved before the Investment Analysis Readiness Decision (IARD).

3.2 Overview

Figure C.1 shows possible inputs into an OSA as well as the basic OSA components: The Operational Services and Environment Description (OSED), the Operational Hazard Assessment (OHA), and the Allocation of Safety Objectives and Requirements (ASOR).

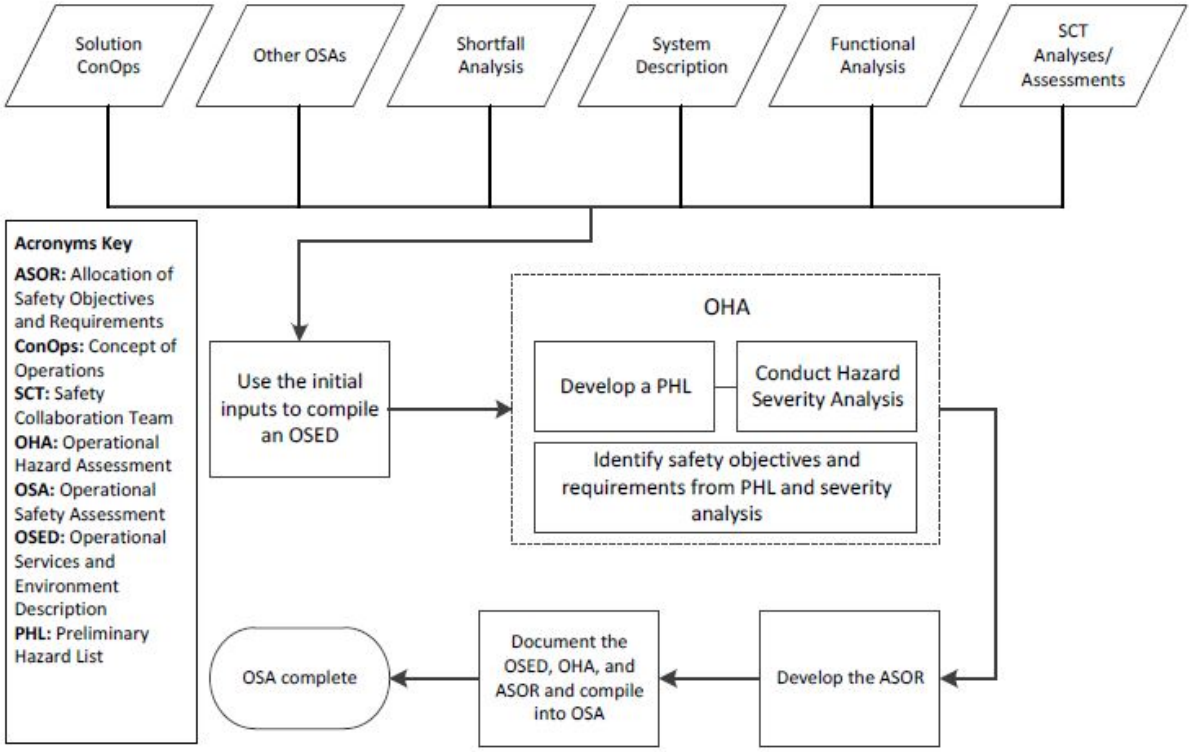

Figure C.1: OSA Inputs and Components

3.3 OSA Components

The OSA components are described as follows:

3.3.1 Operational Services and Environment Description

The OSED describes the service characteristics of the solution concept in an operational environment. This description includes both ground and air elements and must include all the elements of the 5M Model (as discussed in the ATO SMS Manual). The OSED is used as a mechanism platform to describe the service provided by the solution, the users of the solution, and the varying operational and environmental considerations in which the service is provided for the related Communication, Navigation, Surveillance (CNS) and Air Traffic Management (ATM) system. The description provided by the OSED is used as a baseline and solution boundary from which to conduct the safety assessment.

3.3.2 Operational Hazard Assessment

The OHA assesses the operational hazards associated with the shortfall described in the OSED. It determines the severity of each hazard in order to decide operational objectives and safety requirements for any solution that results in an acceptable level of safety risk being achieved when deployed.

3.3.3 Allocation of Safety Objectives and Requirements

The operational objectives and safety requirements identified in the OHA form the basis for assessing the safety of any developed solution. For OSAs conducted across multiple domains, the ASOR allocates the safety objectives and requirements to the service level (e.g., Air Traffic Services or the Flight Standards Service), develops and validates risk mitigation strategies shared by multiple organizations, and allocates safety requirements to those organizations. For OSAs conducted within a domain, or at a distributed level, the ASOR allocates the mitigations and controls to their respective disciplines (e.g., equipment specification, procedure requirements, training, logistics, and maintenance).

3.4 Use of Results

The results of the OSA are used as input to various documents.

3.4.1 Preliminary Requirements

Existing controls and safety requirements identified through the OSA process must be included in the preliminary Program Requirements Document (pPRD). The pPRD must include a requirement for Development Assurance Levels in accordance with ATO-SG-14-01. Other preliminary requirements, such as new/modified air traffic control procedures, Code of Federal Regulations changes, and training, must be separately documented.

3.4.2 Safety Risk Management Documents

The output of the OSA is used as input for Safety Risk Management Documents that must be developed as the solution is further developed (e.g., Comparative Safety Assessment, Preliminary Hazard Analysis, or System Hazard Analysis).

3.4.3 Safety Risk Verification Table

The Safety Risk Verification Table contains all of the safety requirements identified, starting with the origin of the requirement (including those identified in the OSA).

4 Procedures

4.1 Inputs

The following are examples of inputs into the OSA:

4.1.1 Solution Concept of Operations

The Solution Concept of Operations (ConOps) paints a picture of the ideal solution to an identified need or shortfall. It describes how users will employ the new capability within the operational environment and how it satisfies the service need. This document includes descriptions of the characteristics of the proposed solution, the environment in which the solution will operate, and the responsibilities of the users. The Solution ConOps provides information needed for developing the OSA.

4.1.2 SCT-Mandated Safety Analyses or Assessments Reports

These reports provide higher-level information possibly relevant to the OSA. This information may include proposed safety requirements and candidate hazards specifically targeted to the increment that the OSA is addressing.

4.1.3 OSED

Although the OSED is described within this guidance as an element of the overall OSA, one may already be developed as part of a Solution ConOps or an SCT-mandated analysis or assessment. If so, it may be used as input or be further developed for this OSA.

4.1.4 Functional Analysis

A Functional Analysis (FA) examines the functions and sub-functions of a solution that accomplish the operation or mission. An FA describes what the solution does (not how it does it) and is conducted at a level needed to support later synthesis efforts. Products from the FA such as the Functional Flow Block Diagram (FFBD) and N-Squared (N^2) diagram may be used as inputs in developing the OSA. Other techniques may also be used to diagram solution functions.

The outcome of the FA process is a functional architecture. Since the functional architecture may be further refined during the Investment Analysis phase of the AMS lifecycle, a stable FA at even a high level may not be available long enough before the IARD to act as a meaningful enabling input to the OSA. Given that, the OSA should address the solution using either a preliminary or initial functional architecture knowing that it may change as the FA is developed in parallel with the OSA prior to the IARD.

4.1.5 Other OSAs

The legacy NAS is a “System of Systems,” providing multiple services to users. With NextGen, the NAS is evolving into an even more complex configuration. Future acquisitions are beginning to blur the lines of a “system” with defined/fixed boundaries and interfaces. Systems, programs, and projects no longer have unique or exclusive functionality. In fact, the functionalities not only overlap but also may build on one another, subsume each other, or combine for a joint function or capability. Thus, there must be a consistency of safety assessments across hierarchical levels from the program or system level up to the NAS level. Interactions and interdependencies across organizations, operational capabilities, NextGen Portfolios, Operational Improvements, increments, and individual programs or solutions must be addressed in the OSA. Thus, OSAs developed for other solutions/capabilities may be important inputs to an OSA.

4.1.6 Shortfall Analysis

A Shortfall Analysis describes the difference or shortfall between the current service and the desired service. The Shortfall Analysis Report is refined and updated before the IARD. It quantifies the problem as well as its nature, urgency, and impact in operational terms (e.g., airborne or ground delays, accident rate) and describes the potential benefits of the initiative and what improvements in service that could be expected. The Shortfall Analysis Report may provide information useful in identifying potential hazards in an OSA.

4.2 OSED Development Process

The OSED captures elements that comprise a defined CNS/ATM system such as aircraft equipage, air traffic service provider technical systems, communication service provider systems, and procedural requirements and includes the operational performance expectations, functions, and selected technologies of the CNS/ATM system. The OSED facilitates the formulation of technical and procedural requirements based on operational expectations and needs.

Figure C.2 gives a logical overview of the steps required to conduct an OSED. Some of the steps may overlap or be iterative in nature.

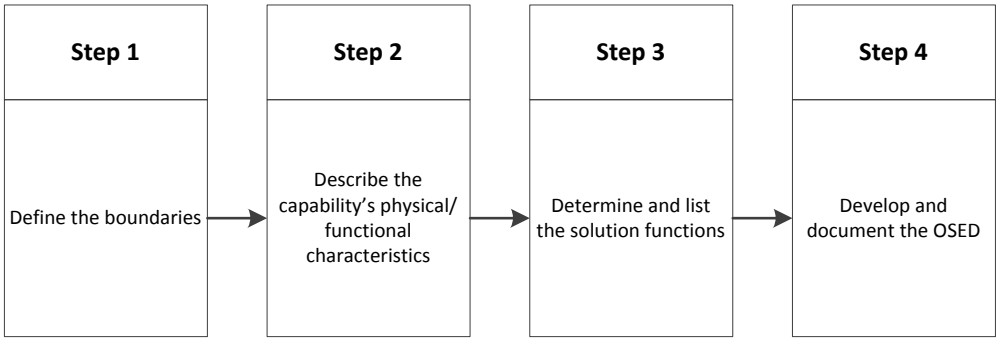

Figure C.2: OSED High-Level Process

The following are required tasks for preparing an OSED.

4.2.1 Define the Boundaries

Define the boundaries of the solution under consideration, including anticipated interfaces, technology independent layers, and common services among NAS systems and sub-systems (both internal and external). Determine, separate, and document which elements of the solution to describe and analyze for hazard identification. Identify shared resources (if any) for which independent SRM was already performed.

4.2.2 Describe the Physical and Functional Characteristics of the Concept

Using models such as those described in the ATO SMS Manual (e.g., the 5M Model), describe the concept's state including physical and functional characteristics, the environment's physical and functional characteristics, air traffic services, human elements (e.g., pilots and controllers, maintenance personnel, supervisors), and operational procedures.

4.2.3 Determine and List Functions

Using the concept description and preliminary input from the FA, determine and list the required functions (including those that are performed by the users). For example, the primary function of a precision navigation system is to provide air traffic control and flight crews with vertical and

horizontal guidance to the desired landing area. If desired, these functions could be split into vertical and horizontal guidance. Supporting functions would be those that provide the solution with the ability to perform the primary function. A supporting function of the precision navigation system would be transmission of the radio frequency energy for horizontal guidance. The PST must determine how to group these functions and to what level to take the analysis.

4.2.4 Develop and Document the OSED

Develop and document the OSED from the information obtained in the first three steps.

4.3 OHA Development Process

Once the solution has been bounded and described and the functions have been identified in the OSED, an SRM panel must determine the associated hazards via an OHA.[4] In developing an OHA, the panel must develop a Preliminary Hazard List (PHL)[5] using a systematic analysis of solution functions and functional failures to identify hazards. Then, each hazard must be classified according to its potential severity after considering causes and effects. The OHA uses the determined severity of each hazard to decide safety objectives and safety requirements for the solution that result in an acceptable level of safety risk being achieved.

In general, as severity increases, the safety objectives and safety requirements must be designed to achieve the lowest possible likelihood of occurrence. A safety objective (i.e., goal) in the context of the OHA is the desire to reduce the likelihood of an identified safety hazard. The associated safety requirement (i.e., minimum level of acceptable performance) is the means of attaining that objective. The OHA must establish safety objectives that ensure an inverse relationship between the probability of a hazard leading to an incident or accident and the severity of occurrence. The safety objective should result in the lowest practicable acceptable level of safety risk.

The OHA may be performed using either qualitative or quantitative methods. However, it is preferable to use quantitative data to support the assessment.[6] Figure C.3 provides an overview of the steps required to conduct an OHA.

4. The ATO SMS Manual provides guidance on how to assemble SRM panels and facilitate the panel process.

5. The concept of the PHL is explained in the ATO SMS Manual.

6. Various databases have been developed to support the SMS. Some of these are listed in Section 8 of the ATO SMS Manual.

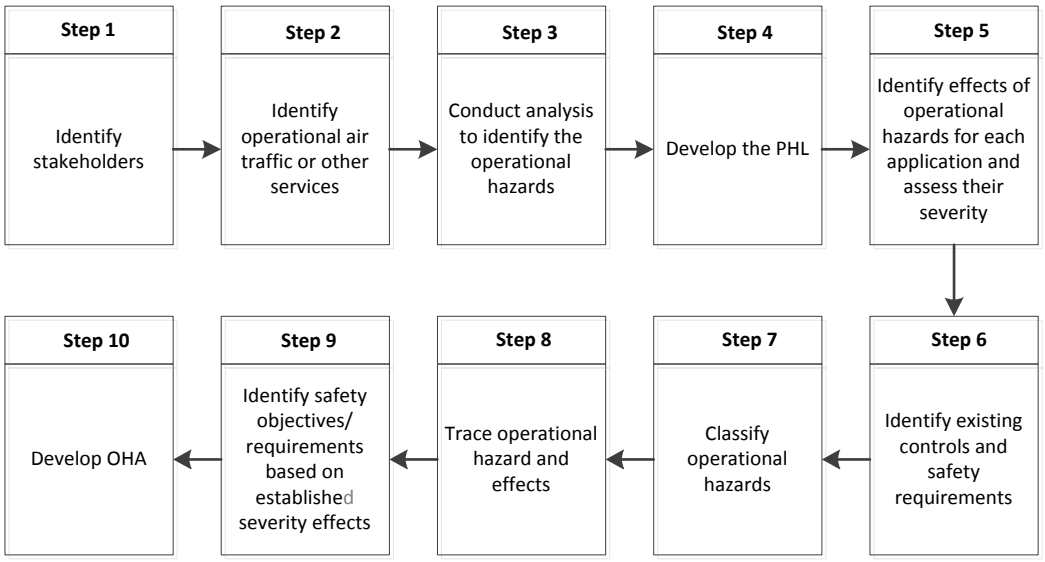

Figure C.3: OHA High-Level Process

The following tasks are required for preparing an OHA:[7]

4.3.1 Identify Stakeholders

Identify applicants, approval authorities, and stakeholders needed to establish and demonstrate compliance with requirements for the air traffic service provision, its use, and any related CNS/ATM system. The stakeholders should also be SRM panel members, as practicable.

4.3.2 Identify Operational Air Traffic or Other Services

Copy the services provided by the solution that were documented in the OSED into the OHA.

4.3.3 Conduct Analysis to Identify the Operational Hazards

Identify the operational hazards. Document the analyses that were undertaken, drawing the linkage between the proposed improvement and the operational safety of the NAS elements, specifically the detailed, logical, and analytical connections. For these types of assessments, the most effective method is to "fail" each of the identified functions and their outputs. This is best done by "failing" the functions from the developed N^2 diagram or the FFBD, if available.

4.3.4 Develop the PHL

Review the hazards identified and develop a PHL that is concise, clear, and understandable; this PHL serves as the repository of the initial efforts of the SRM panel to identify all possible hazards. The PHL is refined and matured over time as the SRM panel validates those identified hazards as credible and the OHA is further developed. The Bow-tie Model[8] may be used as a model to differentiate among hazards, causes, and effects, within the PHL.

7. Refer to the ATO SMS Manual for descriptions of some of the concepts in this section, including a list of analysis tools, the safety order of precedence when determining controls to mitigate the risk of the hazard, determination of safety requirements, and the determination of a hazard's severity.

8. The Bow-tie Model is a diagrammatic illustration of the hazard, the undesirable event, the trigger events/threats and potential outcomes, and the risk controls put in place to minimize the risk. The methodology is an excellent way of visualizing risk management and communicating the context of the controls (barriers and mitigations) put in place to manage risks.

4.3.5 Identify Existing Controls and Safety Requirements

Determine the existing controls; the rationale for their use; and any supporting data that confirm the control's use, applicability, and feasibility related to the hazard under consideration. Controls are measures, design features, warnings, and procedures that already mitigate credible outcomes (i.e., they have already been validated and verified as being effective). They may include procedural requirements, as well as aircraft or ground system requirements related to the solution under review. The Bow-tie Model (specifically the event tree side) can be used for identifying existing controls and safety requirements.

4.3.6 Identify Operational Hazard Effects

Determine the effects of each operational hazard by evaluating the services in the solution state (including legacy system considerations) for the intended operational capabilities, as defined in the OSED. The Bow-tie Model (specifically the outcome side) can be used for identifying effects.

4.3.7 Classify Operational Hazards

Classify each operational hazard according to the severity of its identified effects using the current version of the ATO SMS Manual. The SRM panel must assess all effects of the hazard on operations, taking into account the aircrew, the aircraft, and air traffic services when determining severity and must use the measure yielding a higher severity (i.e., the most conservative estimate). This enables safety objectives and safety requirements to be given a consistent and objective meaning.

The severity of each hazard is determined by the worst credible outcome or effect of the hazard on the solution or the NAS. The severity must be determined using a Bow-tie Model or any other analysis tool, as appropriate.

4.3.8 Identify Safety Objectives

Establish overall safety objectives (either qualitative or quantitative) based on the operational hazard classifications. Once the safety objective is determined for each hazard, safety requirements can be written to ensure that the appropriate hazard controls are established as product requirements. Note that a requirement is a description of what must be done to achieve an objective.

4.3.9 Develop an OHA Worksheet

Document the OHA by populating an OHA worksheet with information for all the identified hazards and their associated safety objectives and safety requirements. The worksheet categories are described in Figure C.4.

Table C.1: OHA Worksheet Categories

Hazard Name	Hazard Category	Hazard Description	Cause Category	Solution State
Create a unique name for the hazard	Note the category of the hazard being assessed: • Controller error • Equipment (software or hardware) malfunction • Pilot/operator error • Runway/airport hazard • Lack of communication • Environmental factors • Other (specify)	Specifically describe the hazard	Describe the primary cause category most closely related to one of these broad categories: • Controller • Pilot • Technician • Equipment (software or hardware) • Obstacle • Airframe • Environment • Other (specify) Further describe the primary human cause using one or more of these sub-causes: • Situational awareness • Workload • Complacency • Compliance • Understanding • Experience • Communications • Distraction • Fatigue • Other (specify)	Describe the significant solution state limitations within one or more of these broad categories: • Weather constraints • Traffic demand • Runway/airport acceptance • Route availability • Airspace saturation • Equipment malfunction/failure • Unconstrained • Other (specify)
Existing Control	**Effect Type**	**Severity**	**Severity Rationale**	**Safety Objectives**
Describe each existing control within one of these broad categories: • Equipment design/function • Regulatory requirement • Policy/procedure • Best practice • Work aid • Other	Describe the effect type within one of these broad categories: • Proximity event • Runway incursion • Risk analysis event • Reduction in safety margin • Flight crew impact • Discomfort/injury/ fatality to passengers • Air Traffic Control workload • Exceeding airframe parameters • Other (specify)	Using the risk matrix in the SMS Manual, assign the hazard effect a severity level from 1 to 5	Give a descriptive rationale for the severity level assigned	Describe the safety objective to potentially mitigate the risk of the identified hazard to an acceptable level

4.4 ASOR Development Process

In the ASOR, safety requirements are developed to achieve the safety objectives identified in the OHA. Safety objectives and safety requirements must then be allocated to the CNS/ATM system elements that provide the functional capability to perform the service and to the stakeholders in control of or responsible for each of the elements. Safety objectives and requirements must be further synthesized into the appropriate standards and specifications, which are used by the FAA/ATO to ensure that systems are compliant.

The ASOR uses the safety objectives and requirements developed and derived from the OHA to develop a strategy that takes into account procedural and architectural mitigations. The set of safety requirements to meet the objectives are allocated to the various ground and/or airborne CNS/ATM systems.

Figure C.4 provides an overview of the steps required to compile an ASOR.

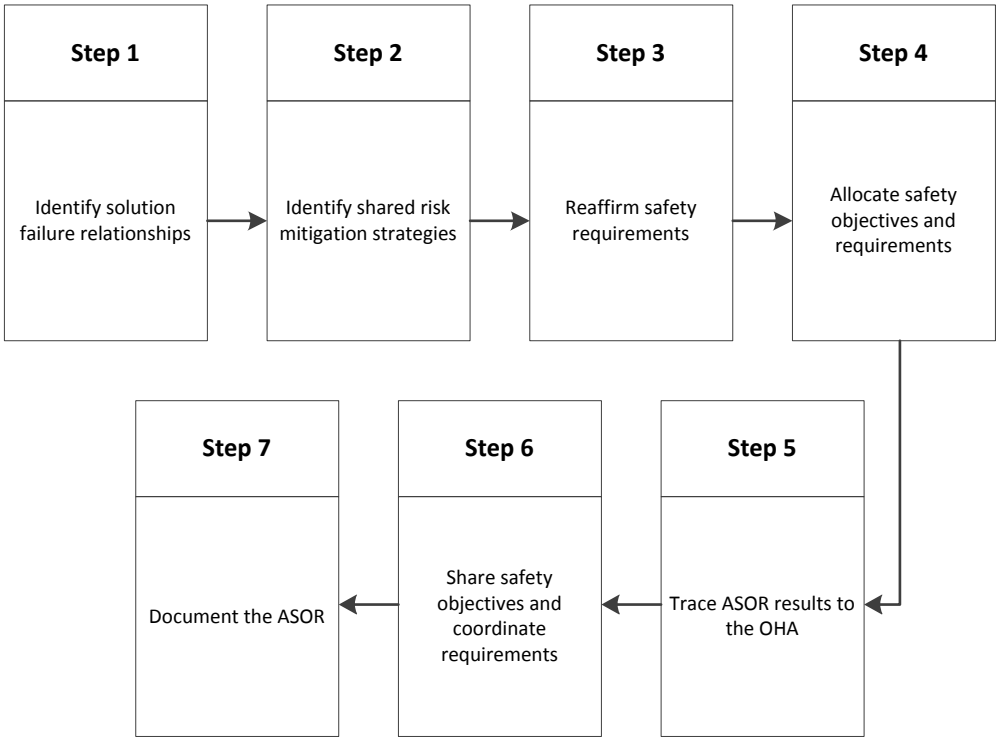

Figure C.4: ASOR High-Level Process

The following steps are required for preparing an ASOR:

4.4.1 Identify Solution Failure Relationships

Identify the relationships between CNS/ATM solution failures, procedural errors, and their effects on air traffic services and the hazard. Include identification of common cause failures and errors occurring among elements of the solution.

4.4.2 Identify Shared Risk Mitigation Strategies

Identify risk mitigation strategies that are shared by multiple elements of the CNS/ATM solution, including mitigation of effects from common cause failures and errors occurring across solution elements. CNS/ATM solution mitigation includes architectural and procedural aspects of the

solution, as well as environmental mitigation and related candidate safety requirements identified in the OHA.

4.4.3 Develop and Reaffirm Safety Requirements

Reaffirm that the safety requirements developed from the shared risk mitigation strategies satisfy the safety objectives. The safety requirements identified must be complete, concise, clear, and necessary at the product level.

4.4.4 Allocate Safety Objectives and Requirements

Allocate the safety objectives and safety requirements, including safety requirements from environmental mitigation, to elements of the CNS/ATM solution. (These requirements should be included in the pPRD.) The allocations may require updating based on feedback from other processes (e.g., safety requirements from other OSAs or Memoranda of Understanding between the ATO and the FAA Office of Aviation Safety). Allocations may also require updating based on an organization's rejection of responsibilities initially assigned by the OSA. Understanding the interactions of air traffic procedures and airspace characteristics assist in the identification of failures, errors, and combinations of both that contribute significantly to the hazards identified in the OHA.

4.4.5 Trace the ASOR Results to the OHA

Trace the ASOR results to each safety objective identified in the OHA.

4.4.6 Share Safety Objectives and Coordinate Safety Requirements

Coordinate the ASOR results such that:

- The impact of the ASOR on the NAS and other operational assessments is identified and reported.
- The impact of the ASOR on development and qualification of solution elements is identified and reported to the appropriate organizations. This impact includes criteria for quantifying safety objectives, determining development assurance requirements, considering architecture (including design features), and reducing the effects of generic design and implementation errors. Criteria for validating the effectiveness of procedural requirements must also be provided.

4.5 Assemble the OSED, OHA, and ASOR as an OSA and Prepare it for Approval

OSAs must be approved per the guidance of Section 8.5 of the Safety Risk Management Guidance for System Acquisitions. (OSAs that support NAS acquisitions must be submitted to the ATO Chief Safety Engineer for approval.[9]) The OSAs must be uploaded to the SMTS per the instructions in the SMTS User Manual.

4.6 Validate OSA Results

Ensure the correctness and completeness of the safety objectives and requirements, including candidate safety requirements identified during the OHA. This ensures that requirements are necessary and sufficient for operational implementation. The validation may include analysis, simulation evaluations, concept testing, and operational trials. The validation includes a consistency check between the safety requirements and the OSED.

9. ANG is the review and acceptance authority for all OSAs prepared for the CRD phase of the acquisition lifecycle. However, an OSA is not required for entrance into this phase.

Appendix D

Guidance for Conducting and Documenting a Comparative Safety Assessment

Guidance for Conducting and Documenting a Comparative Safety Assessment

1 Purpose

This guidance gives a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for conducting and documenting a Comparative Safety Assessment (CSA).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the system engineering processes referred to are described in the National Airspace System (NAS) System Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS Section 4.12, National Airspace System Safety Management System
- ATO SMS Manual
- ATO Order JO 1000.37
- NAS SEM
- Safety Management Tracking System (SMTS) User Manual
- ATO Safety Guidance (ATO-SG) 14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*

3 Background

3.1 Description

A CSA provides management with a level comparison of all the identified potential safety hazards associated with meeting competing sets of operational requirements for alternate solution approaches and architectures. It provides a more detailed safety risk assessment for each proposed investment alternative being considered and builds upon the assessments of likelihood of events identified in the previously conducted Operational Safety Assessment (OSA). Some alternatives that were not viable may have been discarded prior to this point. The remaining alternatives must now be complete, diverse, and technically viable.

The alternatives assessed may range from the reference case[1] of maintaining the status quo to implementing new designs, procedures, or program operational changes. The CSA determines the acceptability of each alternative from a safety risk perspective to allow informed and data-driven decisions by FAA management. Other considerations in making a final alternative

1. Before differences brought about by a proposed change may be fully understood, the “reference case” must be stated. The reference case provides conditions as they are, or would become, if the proposed change is not accepted. The reference case provides a contextual basis to see and compare differences over time. More than a snapshot of the “before” state, the reference case must logically progress and carry forward known assumptions, constraints and smart, independent evolutions, minus the proposed change to make visible the size, number, and magnitude of capability holes the proposed change might fill.

decision include cost, schedule, outside interdependencies, and training, but they are not within the scope of a CSA. Those considerations are discussed in the Investment Analysis Plan or in Business Case Reports. CSAs are typically conducted by the Program Management Organization (PMO) in-house, assisted by the Program Safety Team (PST).[2]

The Initial Investment Decision (IID) is the point at which the Joint Resources Council (JRC) approves or selects the best alternative that both meets the required performance and offers the greatest value to the FAA and its stakeholders. To support the IID, the PMO must complete a CSA and, through Safety and Technical Training (AJI),[3] inform the JRC of the safety risk acceptability of each alternative.

A CSA is related to but different from an OSA. Whereas an OSA defines the target level of safety irrespective of the solution, a CSA provides an estimation of the potential safety risk associated with each proposed solution alternative.

3.2 Overview

The CSA is a risk assessment that defines severity and likelihood of the initial and predicted residual risk of each proposed alternative. The CSA builds upon an OSA (if one was previously conducted) by using the top-level Functional Analysis (FA) that was developed before the OSA. The FA is decomposed at least one more level in order to further expand the Preliminary Hazard List (PHL)[4] produced in the OSA. If an FA has not been previously developed, the PMO must develop one as input to the CSA. If an OSA has not been previously conducted, then the PMO must develop a PHL in the CSA. Figure D.1 provides an overview of the CSA development process.

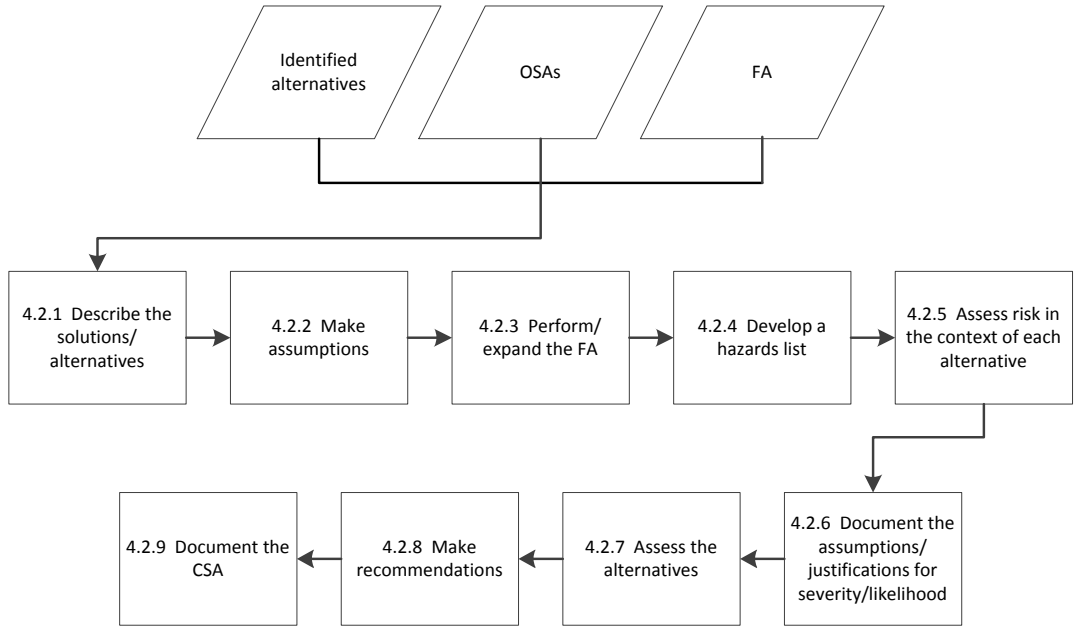

Figure D.1: The CSA Development Process

2. A PST is a resource provided by the PMO to support the safety efforts of the acquisition throughout the AMS lifecycle. The PST is supported by an AJI Safety Case Lead.

3. The ATO Chief Safety Engineer is responsible for this.

4. The concept of the PHL is explained in the ATO SMS Manual.

3.3 Use of Results
The results of the CSA are used as input into the items described below.

3.3.1 Preparing/Revising the Program Requirements Document
Existing controls from the reference case and generic safety requirements identified through the CSA process for each selected alternative (as yet solution agnostic) must be included in the initial Program Requirements Document (iPRD). Related changes by alternative analyses must be separately documented. These changes include preliminary requirements from interdependent investments, new/modified air traffic control procedures, compliance with updates to the Code of Federal Regulations, and lifecycle integrated logistics support (e.g., maintenance, training). At this stage, the iPRD defines the program's needs and requirements at a high level.

3.3.2 Establishing the Development Assurance Level
The Development Assurance Level (DAL) for each alternative (if applicable) is validated in the CSA, as defined by ATO-SG-14-01.[5] (Note: The DAL may differ among the investment alternatives assessed.[6])

3.3.3 Preparing Safety Risk Management Documents
The output of the CSA should be used as input to other Safety Risk Management Documents, particularly, a Preliminary Hazard Analysis (PHA),[7] as the capability/solution alternative pros and cons are debated after the IID.

3.3.4 Preparing/Revising the Safety Risk Verification Table[8]
The Safety Risk Verification Table contains all of the safety requirements identified, starting with the origin of the requirement, and should include those identified in the CSA.

4 Procedures
This section describes the CSA development process.

4.1 Initial Inputs
The following are examples of inputs to the CSA.

4.1.1 Identified Alternatives
Investment analyses should bring at least three diverse yet technically viable alternatives forward for selection of a preferred solution alternative. Ideally, the reference case is not one of these alternatives. Instead, it is a baseline against which the alternatives are compared. Consider the fact that the reference case is not always a "do nothing" scenario, since many legacy program activities may already be in place and go through some default evolution during the required implementation time of the alternative solutions. Therefore, safety aspects of not investing further but letting the existing system continue without the targeted new capability need to be understood to see whether the targeted new capability is an improvement or diminishment to the existing system.

5. This ATO-SG provides instruction for the use of development assurance methods for ground systems software that affects the safety of operations in the NAS and is available on the ATO SMS website.

6. The DAL for the eventually selected alternative is included in the iPRD and the initial Implementation Strategy and Planning Document prior to the Final Investment Decision.

7. A PHA is best compiled after the alternatives are evaluated and a single alternative is selected as the best option. The PHA is conducted after the CSA and before the Final Investment Decision.

8. The final Safety Risk Verification Table is not required until the System Safety Assessment Report is prepared.

4.1.2 Operational Safety Assessments

OSAs previously conducted for IARD may provide relevant information concerning safety hazards, causes, solution states, effects, and severity assessments to the CSA. Using this input in the CSA, the likelihood of each hazard/cause/effect must be determined and matched with severity ratings. Differences among alternatives should begin to emerge, which could impact the combinations of cause/effect severity and likelihood ratings associated with each hazard. Those ratings that are identical across all alternatives drop out as discriminators, leaving those that do differ to be of prime importance to the CSA.

4.1.3 Functional Analysis

A Functional Analysis (FA), as described in the NAS SEM, is used to examine the functions and sub-functions of a system solution that may accomplish the system's operation or mission. An FA describes what the system does (not how it does it) and is conducted at a level needed to support later synthesis efforts. Products from the FA such as the Functional Flow Block Diagram and N-squared diagram (although other techniques may be used to diagram system functions) are further matured as the system's lifecycle progresses and may be used as inputs in developing the CSA. If the alternative solutions are sufficiently diverse, then the functional architectures (as yet solution agnostic) begin to exhibit significant differences that affect safety risk, making the CSA of value. Should no difference in safety risk be determined, the CSA no longer helps to distinguish a preferred alternative, leaving outside business case factors as sole determinants.

Note: The FA is an iterative process that results in an increasingly refined functional architecture. The functional architecture cannot be finalized until the system's final requirements are completely defined. This most likely is after the CSA is performed.

4.2 CSA Development Process

4.2.1 Describe the Solutions/Alternatives

Describe the solutions under study in terms of the 5M Model, per the ATO SMS Manual. At this point, a number of different architectures and alternatives have been identified to meet the operational requirement. Describe each alternative (in sufficient detail to ensure the audience can understand the proposed solution); alternative similarities and differences; and the hazards, causes, effects, and safety risks that may be identified and assessed, with emphasis on the differences.

4.2.2 Make Assumptions Only If Specific Information Is Not Available

As necessary, make assumptions that are conservative in nature and clearly identified. Make them in such a manner that they fairly distinguish among the alternatives which aspects do or do not adversely affect the safety of the solution.

4.2.3 Perform/Expand the FA

Perform an FA (or expand the one previously developed), in accordance with the NAS SEM. Attempt to match similar and unique causes associated with each hazard into a firm list of unique events that may be adequately addressed by existing functions or by postulating new low-level system functions. This analysis results in complete sets of hierarchical functions that alternative system solutions must perform.

Look for matches between system function and mitigation of all causes (within system bounds). Organize causes that fall beyond system bounds into assumptions and constraints for

coordination with external NAS entities. Though all such external dependencies may be noted, it may not be possible to address them within the bounds of this system.

Analyze all external causes that cannot be mitigated within system bounds for faulty assumptions that may invalidate the efficacy of the best solution that could be engineered. Adjust concepts as needed until a good fit is obtained between hazard causes that can be mitigated within this system boundary and operational plans for reaching adequacy of every listed (known) external constraint.

Decide which alternative solutions remain viable after a cursory look at safety. Discard any potential solution "fragments"[9] that inadequately address safety concerns.

4.2.4 Develop a Hazards List

From the FA and solution description, refine and expand as necessary the partial PHL developed in the OSA (assuming an OSA was conducted). If a partial PHL was not previously compiled, then develop one as described in the ATO SMS Manual. Carry over any valid OSA-identified hazards / causes / solution states / severity ratings to the CSA. If any OSA hazards need to be deleted or modified in the CSA, provide a supporting rationale as to why this must be done. Table D.1 presents a sample hazard list that has been expanded/modified from an OSA.

Table D.1: CSA Hazards List

ID	HAZARD	DISPOSITION FOR CSA	VALIDITY/RATIONALE
OSA TFDM-1	Loss of all system functionality	Becomes TFDM-1	Valid hazard
OSA TFDM-2	Loss of electronic flight display	Becomes TFDM-2 with enhanced wording	When updated, needed hazard
OSA TFDM-3	Incorrect flight data display	Becomes TFDM-3	Valid hazard
OSA TFDM-4	Controller fails to pass and/or edit electronic flight strips in a timely and efficient manner	Deleted	Invalid hazard: SRM panel believes the system fails, not the controller
TFDM-X	Xxx xxxx xxxx xxxxx xxxx.	Newly identified	N/A

4.2.5 Assess Risk in the Context of Each Alternative

Evaluate each hazard-alternative combination for risk differences using the definitions and principles contained in the ATO SMS Manual. Evaluate the hazard severity in the context of the worst credible conditions. Remember, severity can and should be defined independently of the likelihood of occurrence. Evaluate the likelihood of occurrence of the hazard conditions resulting in an event at the highest level of severity and not simply the probability of any hazard occurring.

9. NAS services may be composed of many cooperating parts or "solution fragments" in the form of federated systems, sub-systems, or services, all of which must perform with efficient orchestration to achieve some desired operational capability outcome for users. Solution fragments accomplish nothing individually without the rest of the NAS System-of-Systems to complete provision of benefits to end users.

4.2.6 Document the Assumptions and Justifications

Clearly define which adverse events are to be tracked as the best indicators of safety. Identify how to measure adverse events and provide any baseline measures prior to the proposed change, if known. Trace through causes and solution states to arrive at a means of distinguishing those measures that quantitatively (or only qualitatively) support declarations of severity by the Safety Risk Management (SRM) panel. In the early stages of SRM for alternative concepts, there are occasionally solution fragments and less than fully defined systems, making it difficult to assign specific severity and likelihood ratings. Document assumptions and justifications for how severity and likelihood for each hazard condition were determined. Describe whether the alternatives are detailed enough at this stage in development to draw meaningful conclusions about their differences with regard to safety. If additional information is required, describe when and how any deferred analysis reaches a definitive answer, if possible. Describe any new data collection methods required, and identify future decision points at which important measures are likely to be available.

4.2.7 Assess Each Alternative from a Safety Perspective

Assess the acceptability of the safety risk associated with implementation of each alternative under consideration. Document the assessments using Table D.2. (Note: Each alternative assessed has its own table.) Summarize any similarities and note any significant differences. Explain the level of confidence with the outcome by determining a rudimentary level of precision with regard to the possible breadth of range of values that the SRM panel expressed.

Table D.2: CSA Worksheet Categories

Hazard Name	Hazard Category	Hazard Description	Cause Category	Solution State	Existing Control
Create a unique name for the hazard	Note the category of the hazard being assessed: • Controller error • Equipment (software or hardware) malfunction • Pilot/operator error • Runway/airport hazard • Lack of communication • Environmental factors • Other (specify)	Specifically describe the hazard	Describe the primary cause category most closely related to one of these broad categories: • Controller • Pilot • Technician • Equipment (software or hardware) • Obstacle • Airframe • Environment • Other (specify) Further describe the primary human cause using one or more of these sub-causes: • Situational awareness • Workload • Complacency • Compliance • Understanding • Experience • Communications • Distraction • Fatigue • Other (specify)	Describe the significant solution state limitations within one or more of these broad categories: • Weather constraints • Traffic demand • Runway/airport acceptance • Route availability • Airspace saturation • Equipment malfunction/ failure • Unconstrained • Other (specify)	Describe each existing control within one of these broad categories: • Equipment design/function • Regulatory requirement • Policy/procedure • Best practice • Work aid • Other

Effect Type	Severity	Severity Rationale	Likelihood	Likelihood Rationale	Initial Risk Level
Describe the effect type within one of these broad categories: • Proximity event • Runway incursion • Risk analysis event • Reduction in safety margin • Flight crew impact • Discomfort/injury/ fatality to passengers • Air Traffic Control workload • Exceeding airframe parameters • Other (specify)	Using the risk matrix in the ATO SMS Manual, assign the hazard effect a severity level from 1 to 5	Give a descriptive rationale for the severity level assigned	Using the likelihood tables in the ATO SMS Manual, assign the hazard a severity level from A to E	Give a descriptive rationale for the likelihood level assigned	Combine severity and likelihood to determine the initial risk level

4.2.8 Establish Safety Requirements and Predict Residual Risks

For each alternative, establish:

- Preliminary safety issues for tracking in the future;
- Needs, which may become requirements when validated;
- Missing functional requirements needed to turn solution fragment(s) into complete and viable solutions;
- Predicted residual risk levels based on potential and achievable performance minimums should this alternative be selected, designed, fabricated, tested, fielded, and logistically supported for its full lifecycle.

At this point, the CSA may only lay the groundwork to better define a preferred alternative (as yet unselected) that will be better detailed in the PHA. Again, some aspects of relative difference among alternatives may be apparent even if absolute measures of each alternative's suitability against the reference case may not be known.

Intelligently discount and drop out similar unknowns deemed "equal" across each of the alternatives, leaving the known differences as key points of distinction. When completed, the CSA positively impacts the decision-making process by helping to discount several lesser alternatives, indicating one preferred alternative on the basis of clear differences in predicted residual risk. Alternatively, the CSA may return a "no discernible difference" result, leaving subsequent IID decisions to be made on the basis of outside business case factors. Use Table D.3 to tabulate results. (Note: Each alternative assessed has its own table.)

Table D.3: Safety Requirements and Residual Risks

Hazard Name	Initial Risk	Safety Requirement(s)	Predicted Residual Risk

4.2.9 Make Recommendations Based on the Data in the CSA

For decision-making purposes, compare the results of the safety risk assessment of each alternative considered. Compile the results in Table D.4. (Note: Not all hazards may apply to each alternative assessed. Enter "N/A" in Table D.4 when appropriate.) Ensure the decision-makers can clearly distinguish the safety merit of each alternative. Prepare an executive summary that clearly states whether the CSA finds all alternatives alike or whether one or two particular alternatives are clearly superior to others on the basis of safety risk.

Note: The cost of implementing the recommended hazard mitigations identified for each alternative is not a CSA consideration; the safety acceptability of each alternative is the only consideration.

Table D.4: Comparison of Safety Assessments

Alternative	Alternative Description	Risk Rating					
		Hazard 1 Name	Hazard 2 Name	Hazard 3 Name	Hazard 4 Name	Hazard 5 Name	Comments
1							
2							
x							

4.2.10 Document and Assemble the CSA and Prepare it for Approval

CSAs must be approved per the guidance of Section 8.5 of the SRMGSA. The CSAs must be uploaded to the SMTS per the instructions in the SMTS User Manual.

It is particularly important that the hazards and the safety requirements from the CSA be entered into the SMTS so that the PHA (for the eventual preferred alternative) and subsequent verification/validation activities may be tracked once an alternative is down-selected.

4.3 Validate the CSA Results

For typical programs, safety requirements validation of the down-selected alternative is conducted following the Final Investment Decision. Validation ensures the correctness and completeness of the safety objectives and requirements, including candidate safety requirements. This ensures that the safety requirements are necessary and sufficient for operational implementation.

Appendix E

Guidance for Conducting and Documenting a Preliminary Hazard Analysis

Guidance for Conducting and Documenting a Preliminary Hazard Analysis

1 Purpose

This guidance gives a process consistent with the Air Traffic Organization (ATO) Safety Management System (SMS) for conducting and documenting a Preliminary Hazard Analysis (PHA) of the program approved at the Final Investment Decision.

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the system engineering processes referred to are described in the National Airspace System (NAS) System Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS Section 4.12, National Airspace System Safety Management System
- ATO SMS Manual
- ATO Order JO 1000.37
- NAS SEM
- Safety Management Tracking System (SMTS) User Manual
- ATO Safety Guidance 14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*

3 Background

3.1 Description

For systems acquisitions, the PHA[1] is a broad initial hazard identification process conducted by the Program Manager (PM) during the Investment Analysis phase of an acquisition. It is a systematic and detailed hazard analysis of system hardware and software, the environment in which the system exists, and the system's intended use or application. It focuses on the details of the early system design (including possible implications) and is primarily used to perform a safety risk assessment to develop early safety-related requirements and specifications and to support the verification and validation of existing safety requirements. The PHA technique focuses on identifying potential hazards early in the life of a system, thus saving time and money that might be required for major redesign if those hazards were discovered at a later date.

The PHA follows the DIATT (**D**escribe the system, **I**dentify hazards, **A**nalyze risk, **A**ssess risk, **T**reat risk) process identified in the ATO SMS Manual by identifying potential safety hazards, ranking them according to their severity and likelihood, and translating these potential hazards into high-level systems safety design constraints and hazard controls (See Figure E.1).

1. The acronym PHA is used when referring to hardware- and software-related NAS changes. The Hazard Analysis Worksheet (HAW) is the Air Traffic Control procedures equivalent that is used for all other applications. The HAW process is identical to the PHA process.

The output of the PHA is used to develop systems safety requirements and assist in preparing performance and design specifications. In addition, the PHA is often a precursor to more detailed safety risk assessments (e.g., System Hazard Analysis, Sub-System Hazard Analysis), as additional safety analyses are generally required to more fully understand and evaluate safety hazards identified by the Safety Risk Management (SRM) panel. Per the AMS, completion of the PHA is also a requirement for consideration at the Final Investment Decision.

At the time a PHA is conducted, there are few, if any, fully developed system specifications and little or no detailed design information. Therefore, the safety risk assessment relies heavily on the knowledge of Subject Matter Experts. If these experts do not participate on the SRM panel preparing the PHA, or if the system is a new technology having little or no early operational history, the results of the PHA reflects the uncertainty of the panel in many of its assessments and assumptions.

A PHA may be used as a complete safety risk analysis of some systems. This possibility depends both on the complexity of the system and the objectives of the analysis. This is determined by the PM at the Safety Strategy Meeting and reflected in the Program Safety Plan (PSP).

3.2 Use of Results

The PHA results may be used to:

- Identify safety requirements to include in the final Program Requirements Document.
- Highlight important safety risks.
- Identify safety risk issues.
- Identify improvement opportunities and make recommendations concerning the elements of the system that are most likely to contribute to future problems.
- Develop specific suggestions for improving future activity or system performance, including:
    - Equipment modifications,
    - Procedural changes, or
    - Administrative policy changes.
- Develop systems safety requirements by:
    - Preparing design descriptions.
    - Recommending additional safety risk assessments. As suggested by the name, the PHA is conducted in an early phase of a project. The insights gained from the PHA help determine which, if any, additional safety risk assessments should be conducted and serve as input to more detailed safety risk analyses. These recommendations are reflected in the PSP.

3.3 Hazard Analysis Techniques

Refer to the ATO SMS Manual and the NAS SEM, which describe various hazard analysis techniques that may be used in developing a PHA. These techniques include:

- Function Failure Analysis,
- Event Tree Analysis,

- Failure Modes and Effects Analysis,
- Fault Tree Analysis,
- Cause-consequence Diagram, and
- “What if” analysis.

4 Procedures

4.1 Overview

Figure E.1 shows the high-level PHA process.

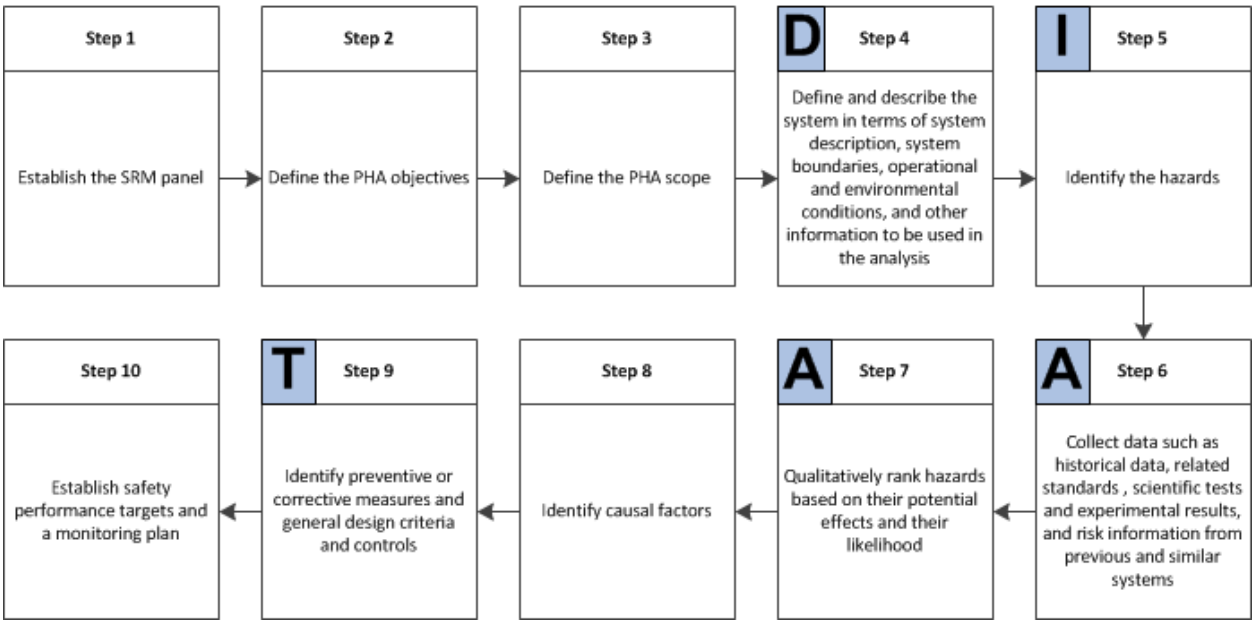

Figure E.1: PHA High-Level Process

4.2 Inputs

The following list describes inputs into the PHA.

- **System Description:** A description of the system under development and the context in which it is to be used including layout drawings, process flow diagrams, and block diagrams.
- **Safety Data:** Historical hazard data (including lessons learned from other systems) that allow the incorporation of experience gained from previous operation of the same system or similar systems. Potential data sources are listed in the ATO SMS Manual.
- **Functional Analysis (FA):** An expansion of the FAs conducted to support the Operational Safety Assessment (OSA) or Comparative Safety Assessment (CSA) conducted earlier in the AMS lifecycle.
- **Preliminary Hazard List:** A list of hazards determined in previous safety analyses or brainstorming.
- **Hazard Checklist:** A list of the causes of safety incidents with the same or similar equipment.

- **Customer Requirements:** Any pre-existing requirements specifications and concept documents.
- **Regulatory Requirements:** Constraints imposed by regulatory agencies.
- **Previously Conducted Safety Analyses:** Any relevant information from safety assessments (e.g., OSAs or CSAs) already conducted.

4.3 Content

The PHA must be written in accordance with the requirements of the ATO SMS Manual and the Safety Risk Management Guidance for System Acquisitions (SRMGSA). The description of each identified hazard must contain, at a minimum, the information presented in Table E.1.

Table E.1: Components of a PHA

Hazard Name	Hazard Category	Hazard Description	Cause Category	System State	Existing Control
Create a unique name for the hazard.	Note the category of the hazard being assessed: • Controller error • Equipment (software or hardware) malfunction • Pilot/operator error • Runway/airport hazard • Lack of communication • Environmental factors • Other (specify)	A hazard is any real or potential condition that can cause injury, illness, or death to people; damage to or loss of a system, equipment, or property; or damage to the environment. It is a condition that is a prerequisite to an accident or incident. Specifically describe the hazard in a complete statement.	Causes are events that result in a hazard or failure. Causes can occur by themselves or in combinations. They may include, but not be limited to, human error, latent failure, active failure, design flaw, component failure, and software error. Describe the primary cause category most closely related to one of these broad categories: • Controller • Pilot • Technician • Equipment (software or hardware) • Obstacle • Airframe • Environment • Other (specify) Further describe the primary human cause using one or more of these sub-causes: • Situational awareness • Workload • Complacency • Compliance • Understanding • Experience • Communications • Distraction • Fatigue • Other (specify)	System state is an expression of the various conditions, characterized by quantities or qualities, in which a system can exist (e.g., adverse weather and lighting conditions, such as day, dusk, and night). The system state also includes the activity under which the harm may occur (e.g., storage, shipping, installation, testing, maintenance, replacement, decommissioning, or phase of flight). A hazard assessment must consider all possibilities while allowing for all system states, especially when the end results lead to the application of different mitigations. System state must be defined in accordance with the ATO SMS Manual and using one or more of these broad categories: • Weather constraints • Traffic demand • Runway/airport acceptance • Route availability • Airspace saturation • Equipment malfunction/ failure • Unconstrained • Other (specify)	These are the existing safeguards, safety features, protective devices, warnings, training, and procedures that control or eliminate safety risk. An existing safety control is a requirement that exists currently in the FAA (e.g., a control that was previously defined in a prior analysis) that is validated or verified to mitigate or manage the safety risk of a hazard's effect or occurrence. Describe each existing control within one of these broad categories: • Equipment design/function • Regulatory requirement • Policy/procedure • Best practice • Work aid • Other

Table E.1: Components of a PHA

Existing Control Justification	Effect Type	Severity	Severity Rationale	Likelihood	Likelihood Rationale
Explain how existing controls were validated and verified.	An effect is the real or credible harmful outcome(s) that can be expected if the hazard occurs in the defined system state. Describe the effect type within one of these broad categories: • Proximity event • Runway incursion • Risk analysis event • Reduction in safety margin • Flight crew impact • Discomfort/injury/ fatality to passengers • Air Traffic Control workload • Exceeding airframe parameters • Other (specify)	Severity is the measure of how bad the results of an event are predicted to be. It is determined by the worst credible outcome. Less severe effects may be considered analytically in addition to this, but at a minimum, the most severe effects are to be considered. Determination of severity is independent of likelihood. Using the risk matrix in the SMS Manual, assign the hazard effect a severity level from 1 to 5.	Provide a descriptive rationale for the severity level assigned.	Likelihood is an expression of how often an event is expected to occur. Severity must be considered in the determination of likelihood. Likelihood is determined by how often the resulting harm can be expected to occur at the worst credible severity. When determining likelihood, the worst credible system states usually determine the worst credible severity. Using the likelihood tables in the ATO SMS Manual, assign the hazard a severity level from A to E.	Provide a descriptive rationale for the likelihood level assigned.

Initial Risk Level	Recommended Safety Requirements	Organization Responsible for Implementing Safety Requirements	Predicted Residual Risk	Safety Performance Targets
Initial risk is the composite of the severity and likelihood of a hazard considering only verified controls and documented assumptions for a given system state. It describes the safety risk at the preliminary or beginning stage of a proposed change, program, or assessment. When assumptions are made, they must be documented as recommended controls. Once the initial safety risk is established, it is not changed.	Safety requirements are suggested mitigations or controls that have the potential to mitigate a safety hazard or risk but have not yet been validated or verified as part of the system or its requirements.	The organization's name and the Point of Contact's name and number must be listed.	Predicted residual risk is the term used until the safety analysis is complete and all safety requirements have been verified. It is based on the assumption that all safety requirements will be validated and verified.	See the ATO SMS Manual for information concerning safety performance targets.

4.4 PHA Documentation and Preparation for Approval

The information in Table E.1 must be used as input to the SMTS, which generates the PHA documentation. Instructions for entering information into the SMTS are in the SMTS User Manual. PHAs must be reviewed in accordance with the peer review process described in Section 8.4 of the SRMGSA and approved per the guidance given in Section 8.5 of the SRMGSA.

Hazards and safety requirements from the PHA must be entered into the SMTS so that subsequent verification/ validation activities may be tracked and monitored.

Appendix F

Guidance for Conducting and Documenting a Sub-System Hazard Analysis

Guidance for Conducting and Documenting a Sub-System Hazard Analysis

1 Purpose

This guidance describes the Sub-System Hazard Analysis (SSHA), which is an update to a Safety Risk Management document that is consistent with the Air Traffic Organization (ATO) Safety Management System (SMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the system engineering processes referred to are described in the National Airspace System (NAS) System Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS Section 4.12, National Airspace System Safety Management System
- ATO SMS Manual
- ATO Order JO 1000.37
- NAS SEM
- Safety Management Tracking System (SMTS) User Manual
- ATO Safety Guidance 14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*

3 Background

3.1 Overview

The SSHA is an important part of any system safety program.[1] It is performed by the system developer in the early stages of Solution Implementation when system design details are known. The SSHA determines how operational or functional failures of components (or any other anomaly) adversely affect the overall safety risk associated with possible outcomes of the system being used in the NAS. It addresses safety hazards in sub-systems by conducting a detailed analysis that identifies hazards and recommends solutions.

The SSHA takes the previously identified hazards that originated in the Preliminary Hazard Analysis (PHA) and any other sources, considers the sub-system design and architecture, and refines those hazards through analytical selection, decomposition, and traceability. Sometimes this uncovers new hazards that manifest because of an implementation choice.

The analysis focuses on failure modes as they contribute to hazards at the sub-system level and investigates the detailed interfaces between components for possible conditions leading to

1. For the sake of simplicity, a “system” is considered to be a whole that cannot be divided into independent parts without losing its essential characteristics. A “sub-system” is a constituent part of a system that performs a particular function.

hazards. In addition, it analyzes component and equipment failures or faults and human errors that establish a hazard due to the functioning of the sub-system.

Sub-systems may be a single media type (e.g., electronic, software, or mechanical). In addition, there may be mixed-media sub-systems such as embedded software-hardware systems or electromechanical actuators that require a more integrated SSHA. In either case, the human is considered a component that both receives inputs and initiates outputs within a sub-system

The SSHA is conducted at a greater level of detail than a PHA and is intended to show that the sub-system design meets safety requirements. The analysis is completed by reviewing design drawings, engineering schematics, and specifications. As the system and related sub-systems are further defined and system design changes (including software design changes) are implemented, the system developer should revise the SSHA as necessary.

When the software to be used in conjunction with the sub-system is developed under a separate software development effort, the system developer performing the SSHA monitors, obtains, and uses the output of each phase of the formal software development process to evaluate the software contribution to the SSHA. Identified hazards that require mitigation action by the software developer must be reported to the Program Management Organization (PMO) to request that appropriate direction be provided to the developers.

Due to the complexity of the SSHA, the analysis is usually identified in a procurement specification and conducted by the system developer. The PMO should include the need to conduct an SSHA as a contractual requirement. A suggested Data Item Description (DID) (AJI-DID-SSHA-001) can be found in the DID Library.

An approved SSHA is required at the In-Service Decision (ISD) review. To support the ISD milestone, the PMO must submit an approved SSHA to Safety and Technical Training.

3.2 Use of the Analysis

An SSHA must:

a) Document sub-system compliance with requirements to eliminate hazards or reduce the associated risks.

   (1) Validate applicable flow-down of design requirements from top-level specifications to detailed design specifications for the sub-system.

   (2) Ensure that design criteria in the sub-system specifications have been satisfied and that verification and validation of sub-system mitigation measures have been included in test plans and procedures.

b) Identify previously unidentified safety hazards associated with the design of sub-systems.

   (1) The implementation of sub-system design requirements and mitigation measures must not introduce any new safety hazards to the system. The PMO must determine potential safety hazards resulting from modes of failure, including:

   - Component failure modes and human errors,
   - Single-point and common cause failures,
   - The effects when failures occur in sub-system components, and

- The effects from functional relationships between components and equipment comprising each sub-system. Consider the potential contribution of sub-system hardware and software events, faults, and occurrences (such as improper timing).

c) Recommend necessary actions to eliminate previously unidentified hazards or mitigate their associated risks.

(1) Determine risk and the need for additional safety requirements to mitigate operational hazards. Develop system safety requirements to assist in preparing performance and design specifications.

(2) Ensure system-level hazards attributed to the sub-system are analyzed and adequate mitigations are identified for possible implementation in the design as directed by the government.

d) Establish the framework for follow-up hazard analyses that may be required.

3.3 Software Aspects of Analysis

Software guidance may be reviewed in the following sections of the Safety Risk Management Guidance for System Acquisitions (SRMGSA):

- Section 6.3, Managing Software Risk;
- Appendix A, Section 4.1.4, Identify Developmental Assurance Requirements;
- Appendix B, Section 3.2.3, Software Development Assurance (for the Investment Analysis Readiness Decision);
- Appendix B, Section 4.2.3, Software Development Assurance (for the Initial Investment Decision);
- Appendix B, Section 5.2.7, Software Development Assurance (for the Final Investment Decision); and
- Appendix B, Section 6.2.7, Software Development Assurance (for the ISD).

The Development Assurance Level (DAL) is based on hazards identified during the Safety Risk Management process. The process to this point was conducted without any details of the implementation and thus had to work on assumptions about how the system would behave. As part of the sub-system, the software is addressed in the SSHA by the system developer. Individuals performing an analysis on the system may not necessarily be experts in software behavior. In addition, the software developer may be a subcontractor to the system developer. Thus, it is critical that the SSHA process address how the software analysts and system analysts communicate and understand each other. The software aspects of hazard analysis must ensure the people doing the safety analysis know enough about the software implementation details to ensure the safety analysis is still valid and are not surprised by an unexpected implementation method. Some may use the term “software hazard analysis,” but it is actually just the software portion of the system analysis. The SSHA is used to validate the assumptions made in the PHA.

The choice of software design and architecture can invalidate current safety requirements and pose new unanticipated hazards that could generate new safety requirements that may affect the DAL. For example, architectural mitigation and partitioning techniques may be used in order

to reduce the DAL. If DAL reduction is proposed, then the PMO must be informed to ensure the reduction can be evaluated and approved.

The SSHA process is iterative, beginning as a preliminary analysis early in the design development. It matures to eventually document the state of the final system. Early in development planning, the SSHA can:

- Develop software safety design constraints,
- Identify specific software safety requirements, and
- Devise software and system safety test plans and testing requirements.

As the design progresses, the SSHA will:

- Ensure that the method for software requirements, design, implementation, and corrective actions does not impair or decrease the safety risk associated with the sub-system and evaluate any new safety hazards introduced into the system;
- Design and analyze the human-computer interface;
- Develop safety-related information for operations, maintenance, and training manuals; and
- Evaluate whether potential changes to the software could affect safety.

The SSHA process ensures the system perspective is represented in the software development. As such, it must consider the safety impact of:

- Errors in algorithms, components, modules, routines, and calculations;
- Hazardous conditions (e.g., deadlocking, inappropriate magnitude, multiple event / wrong event environment, out-of-sequence/adverse environment, and inappropriate inputs or outputs);
- Software components whose performance, performance degradation, functional failure, or inadvertent functioning could result in a hazard or whose design does not satisfy contractual safety requirements; and
- Software events, faults, and occurrences (such as improper timing).

The SSHA documents how the software performs its intended function safely. It does this by:

- Ensuring that the safety design criteria identified in the software requirement specifications have been satisfied and
- Ensuring that the implementation choices have been evaluated so no unsafe conditions have been introduced.

3.4 Other Considerations

- The PMO must refer to the program-specific Program Safety Plan (PSP) approved by the ATO Chief Safety Engineer to determine which safety assessments must be conducted during a systems acquisition.
    - The PMO may use methods other than SSHA to capture required information or may prepare a combined SSHA / System Hazard Analysis to meet AMS requirements only if such alternatives have been approved in the PSP.

- The system safety process is a set of analyses that starts at the PHA and continues through the SSHA, SHA, and Operating & Support Hazard Analysis. Each analysis gets more discrete as more design details are known.
    - The basis of each analysis is a Hazard Analysis Worksheet (HAW). The HAW, initially developed early in the system life cycle (i.e., during the PHA), is further developed, modified, and enhanced as subsequent analyses are conducted.
    - Each subsequent analysis has a slightly different focus but is essentially a HAW that builds on a previously developed HAW.
    - An SSHA is considered to be an update to the previous SRM document prepared for the acquisition system.
- SSHAs are developed for new systems; however, many acquisition programs deploy their capabilities incrementally over time and have an Initial Operating Capability date for each capability. In lieu of a new SSHA, additions to previously developed systems require either updates to existing SSHAs, supplemental hazard analyses, or new hazard analyses. The specifics of such analyses must be defined in the approved PSP.
- Using a commercial-off-the-shelf (COTS) product with a very high reliability as a subsystem or component of a sub-system will not automatically ensure a safe system as reliability does not account for interactions with other system components. This is particularly important to remember with software as it usually controls many, if not all, of the interactions among system components. Simply equating software reliability or specification conformance with safety will not ensure an acceptable safety level of the system. There may be times when it is less expensive and safer to provide special-purpose software rather than a COTS product; using COTS may amount to a false economy.

  There are other times where COTS components may have adequate system safety. In these cases, the producer of that component must provide the prime contractor with either a complete “black box” behavior specification or analysis that shows the component design allows protection against any possible hazardous software behavior; this information must be provided for a complete SSHA to be performed.

4 Preparing the SSHA

4.1 Initial Inputs

Figure F.1 shows some possible inputs to the SSHA.

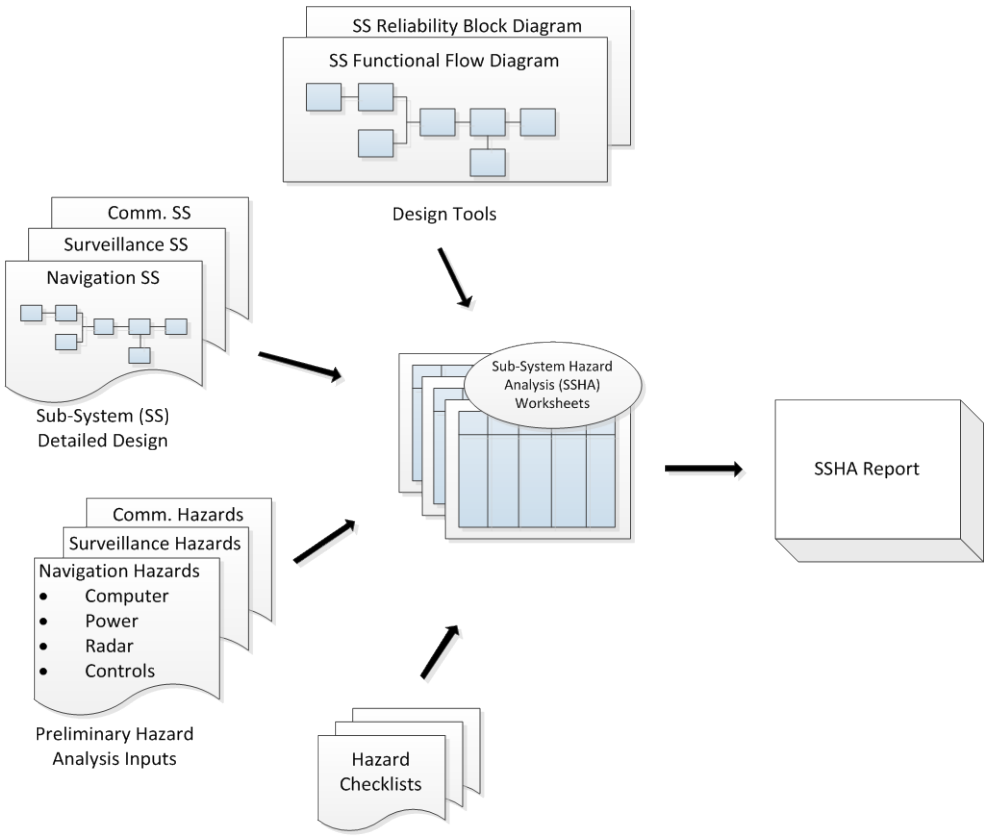

Figure F.1: Inputs to the SSHA

4.2 Hazard Analysis Techniques

Refer to the ATO SMS Manual and the NAS SEM for descriptions of various hazard analysis techniques that may be used in developing a SSHA. These techniques include:

- Function Failure Analysis,
- Event Tree Analysis,
- Failure Modes and Effects Analysis,
- Fault Tree Analysis,
- Cause-Consequence Diagram, and
- "What if" Analysis.

4.3 Conducting the SSHA

The SSHA is essentially a PHA conducted at the sub-system level and should follow the methodology described in the SRMGSA. It is recommended that the SSHA be led by safety engineers with technical proficiency rather than design or system engineers. This is to ensure that the analysis remains a tool to identify hazards and safety issues associated with the design and functional operation of the system and not a defense of the existing design. Design or

system engineers may have difficulty looking away from the sub-system/system designs that they created. The safety engineer must provide a unique, non-parochial view that focuses on potential hazards.

5 Approving the SSHA

SSHAs must be reviewed in accordance with the peer review process in Section 8.4 of the SRMGSA and approved per the guidance in Section 8.5 of the SRMGSA. SSHAs must be uploaded to the SMTS per the instructions in the SMTS User Manual.

6 Preparing and Revising the Safety Risk Verification Table

The Safety Risk Verification Table (SRVT) must contain all of the safety requirements identified (existing, validated, and recommended),[2] starting with the origin of the requirement, and must include those safety requirements identified in the SSHA.

2. The SRVT should include recommended safety requirements that the Program Manager declined to implement.

Appendix G

Guidance for Conducting and Documenting a System Hazard Analysis

Guidance for Conducting and Documenting a System Hazard Analysis

1 Purpose

This guidance describes the System Hazard Analysis (SHA), which is an update to a Safety Risk Management Document that is consistent with the Air Traffic Organization (ATO) Safety Management System (SMS).

2 Applicable Policy and Related Documents

This guidance does not constitute a change to any requirements contained in Federal Aviation Administration (FAA) orders. It supplements and reflects updates to the ATO SMS Manual, which provides guidance on fulfilling requirements set forth in the current version of ATO Order JO 1000.37, *Air Traffic Organization Safety Management System*. This guidance also supplements the FAA Acquisition Management System (AMS). Additionally, the system engineering processes referred to are described in the National Airspace System (NAS) System Engineering Manual (SEM).

The primary reference materials in this guidance are the current editions of the following:

- AMS Section 4.12, National Airspace System Safety Management System
- ATO SMS Manual
- ATO Order JO 1000.37
- NAS SEM
- Safety Management Tracking System (SMTS) User Manual
- ATO Safety Guidance 14-01, *Development Assurance for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*

3 Background

3.1 Overview

The SHA is a safety assessment that the system developer conducts to analyze system operation, system interactions, and system interfaces. It is initiated during the Solution Implementation phase and consolidates and builds upon the Sub-System Hazard Analysis (SSHA) and the Preliminary Hazard Analysis (PHA).[1] The SHA identifies new hazards at system and sub-system interfaces and documents previously unidentified hazards. Ideally, the SHA identifies hazards and safety risks that were not identified in the SSHA as well as hazards and safety risks that apply to more than one sub-system.

The SHA, considering the system as a whole, analyzes the following areas that could contribute to system hazards:

- System operation,
- Interfaces and interactions between sub-systems,
- Interfaces and interactions between the system and sub-systems,
- Interfaces and interactions between the system and external systems,
- Interfaces and interactions between the system and operators, and

1. See Appendix E of the Safety Risk Management Guidance for System Acquisitions (SRMGSA).

- Component failures and normal (correct) behavior.

Safety design requirements (some of which were generated during the PHA) that are included in the final Program Requirements Document are refined during the SHA; the system must be validated for conformance to these requirements. Through the SHA, safety design requirements are traced to individual components based on functional decomposition and allocation. As the system design matures, the SHA should be updated.

The Program Management Organization (PMO) must refer to the program-specific Program Safety Plan (PSP) approved by the ATO Chief Safety Engineer to determine which safety assessments must be conducted during a systems acquisition. The PMO may use methods other than an SHA to capture required information or may prepare a combined SSHA/SHA to meet AMS requirements only if such alternatives have been approved in the PSP.

SHAs are developed for new systems; however, many acquisition programs deploy their capabilities incrementally over time and have an Initial Operating Capability date for each capability. In lieu of a new SHA, additions to these previously developed systems may require updates to existing SHAs, supplemental hazard analyses, or new hazard analyses. The specifics of such analyses must be detailed in the approved PSP.[2]

Due to the complexity of the SHA, the analysis is usually identified in a procurement specification and conducted by the system developer. The PMO should include the need to conduct an SHA as a contractual requirement. A suggested Data Item Description (DID) (AJI-DID-SHA-001) can be found in the DID Library.

An approved SHA is required at the In-Service Decision (ISD) review. To support the ISD, the PMO must submit an approved SHA to Safety and Technical Training.

3.2 Use of the Analysis

An SHA assesses the risks associated with the total system design (including software) and, more specifically, the sub-system interfaces. This includes recognizing previously unidentified hazards associated with the sub-system interfaces and system functional faults and determining whether the method of implementing the hardware, software, facility design requirements, and corrective actions has impaired or degraded the safety of the system or introduced any new hazards. An SHA recommends new/modified system requirements to eliminate identified hazards or to control their associated risk to acceptable levels, refines high-level safety design requirements, and provides a comprehensive analysis baseline for subsequent design changes.

4 Analysis Tools

In an SHA, hazard causal analysis[3] is used to refine the high-level safety requirements into more detailed requirements. This process typically requires a model of the system. Causal analysis usually involves a search through the system design for system states[4] or conditions that could lead to system hazards.

2. See Appendix A of the SRMGSA.

3. In simple terms, a causal analysis is a process used to identify why something occurs.

4. Per the ATO SMS Manual, a system state is the expression of the various conditions in which a system can exist. It is important to capture the system state that most exposes a hazard while remaining within the confines of any operational conditions and assumptions defined in existing documentation.

Some examples of analysis tools that may contribute input to the SHA include:

- Fault Tree Analysis,
- Failure Modes and Effects Analysis,
- Event Tree Analysis, and
- Interface Analysis.

5 Preparing the SHA

The methodology for conducting an SHA matches that of a PHA. The SHA follows the DIATT process (**D**escribe the system, **I**dentify hazards, **A**nalyze risk, **A**ssess risk, **T**reat risk) identified in the ATO SMS Manual by identifying potential safety hazards, ranking them according to their severity and likelihood, and translating these potential hazards into high-level safety design requirements and hazard controls.

Inputs into the SHA include:

- Design knowledge,
- Safety hazard knowledge,
- Output from the PHA,
- Output from the SSHA,
- Output from other analysis tools,
- Output of each phase of the formal software development process, and
- Test results.

The SHA may be used to identify:

- Compliance with specified safety design criteria;
- Possible independent, dependent, and simultaneous hazardous events, including system failures, failures of safety devices, common cause failures and events, and system interactions that could create a hazard;
- Degradation in the safety of a sub-system, or the total system, from the normal operation of another sub-system;
- Design changes that affect sub-systems; and
- Effects of reasonable human errors.

6 Approving the SHA

SHAs must be reviewed in accordance with the peer review process described in Section 8.4 of the SRMGSA and approved per the guidance in Section 8.5 of the SRMGSA. SHAs must be uploaded to SMTS per the instructions in the SMTS User Manual.

7 Preparing/Revising the Safety Risk Verification Table

The Safety Risk Verification Table (SRVT) must contain all of the safety requirements identified (existing, validated, and recommended),[5] starting with the origin of the requirement, and must include those safety requirements identified in the SHA.

5. The SRVT should include recommended safety requirements that the Program Manager declined to implement.

Appendix H

Guidance for Conducting and Documenting an Operation and Support Hazard Analysis

(Future appendix)

Appendix I
Guidance for Preparing System Safety Assessment Reports
(Future Appendix)

Appendix J
Acronyms and Abbreviations

AJI	Safety and Technical Training
AJR	System Operations Services
AJT	Air Traffic Services
AJV	Mission Support Services
AJW	Technical Operations
AMS	Acquisition Management System
ANG	Office of NextGen
AOV	Air Traffic Safety Oversight Service
ARP	Office of Airports
ASOR	Allocation of Safety Objectives and Requirements
ATM	Air Traffic Management
ATO	Air Traffic Organization
ATO-SG	Air Traffic Organization Safety Guidance
AVS	Office of Aviation Safety
CNS	Communication, Navigation, and Surveillance
ConOps	Concept of Operations
COTS	Commercial-Off-the-Shelf
CRD	Concept and Requirements Definition
CSA	Comparative Safety Assessment
DAL	Development Assurance Level
DID	Data Item Description
EA	Enterprise Architecture
EOSH	Environmental and Occupational Safety and Health
FA	Functional Analysis
FAA	Federal Aviation Administration
FAST	FAA Acquisition System Toolset
FFBD	Functional Flow Block Diagram
FID	Final Investment Decision
fPRD	Final Program Requirements Document
fTEMP	Final Test and Evaluation Master Plan
GSIP	Generic Site Implementation Plan
HAW	Hazard Analysis Worksheet
IA	Investment Analysis
IAP	Investment Analysis Plan
IARD	Investment Analysis Readiness Decision
IID	Initial Investment Decision
IOA	Independent Operational Assessment
IOC	Initial Operating Capability
ISA	Independent Safety Assessment
ISD	In-Service Decision
ISM	In-Service Management
ISPD	Implementation Strategy and Planning Document
ISR	In-Service Review

ISSA	Integrated System Safety Assessment
iTEMP	Initial Test and Evaluation Master Plan
JRC	Joint Resources Council
LOB	Line of Business
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
OHA	Operational Hazard Assessment
OI	Operational Improvement
ORM	Operational Risk Management
OSA	Operational Safety Assessment
OSED	Operational Services and Environment Description
O&SHA	Operating and Support Hazard Assessment
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PIR	Post-Implementation Review
PM	Program Manager
PMO	Program Management Organization
PMP	Program Management Plan
POC	Point of Contact
pPRD	Preliminary Program Requirements Document
PSAA	Plan for Software Aspects of Approval
PSP	Program Safety Plan
PST	Program Safety Team
pTEMP	preliminary Test and Evaluation Master Plan
RDBM	Risk-Based Decision Making
SCL	Safety Case Lead
SCT	Safety Collaboration Team
SDLC	Software Development Lifecycle
SEM	Systems Engineering Manual
SHA	System Hazard Analysis
SI	Solution Implementation
SME	Subject Matter Expert
SMS	Safety Management System
SMTS	Safety Management Tracking System
SO	Staff Office
SOC	Safety Oversight Circular
SRM	Safety Risk Management
SRMGSA	Safety Risk Management Guidance for System Acquisitions
SRVT	Safety Requirements Verification Table
SSAR	System Safety Assessment Report
SSHA	Sub-System Hazard Analysis
SSM	Safety Strategy Meeting

SSPP	Systems Safety Program Plan
SSW	Safety Strategy Worksheet
V&V	Verification and Validation